



Ruijie RG-S7805C Switches

RGOS Command Reference, Release 11.0(4)B19P1

Copyright Statement

Ruijie Networks©2020

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Thank you for using our products. This manual matches the RGOS Release 11.0(4)B19P1.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://case.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: [service_rj@ruijienetworks.com](https://www.skype.com/people/service_rj@ruijienetworks.com)

Related Documents

Documents	Description
Configuration Guide	Describes network protocols and related mechanisms that supported by the product, with configuration examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.

{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Symbols



Means reader take note. Notes contain helpful suggestions or references.



Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.



System Configuration Commands

1. Command Line Interface Commands
2. Basic Configuration Management Commands
3. LINE Commands
4. File System Commands
5. SYS Commands
6. Time Range Commands
7. HTTP Service Commands
8. Syslog Commands
9. CWMP Commands
10. Monitoring Commands
11. LICENSING Commands
12. Module Hot-plugging Commands
13. Supervisor Module Redundancy Commands
14. USB Commands
15. PoE Commands
16. UFT Commands
17. PKG_MGMT Commands

18. OpenFlow Commands

1 Command Line Interface Commands

1.1 alias

Use this command to configure a command alias in global configuration mode. Use the **no** form of this command to restore the default setting.

alias *mode command-alias original-command*

no alias *mode command-alias*

Parameter Description	Parameter	Description
	<i>mode</i>	Mode of the command represented by the alias
	<i>command-alias</i>	Command alias
	<i>original-command</i>	Syntax of the command represented by the alias

Defaults Some commands in user or privileged EXEC mode have default alias.

Command Mode Global configuration mode.

Usage Guide The following table lists the default alias of the commands in privileged EXEC mode.

Alias	Actual Command
h	help
p	ping
s	show
u	undebug
un	undebug

The default alias cannot be removed by the **no alias exec** command.

After configuring the alias, you can use a word to replace a command. For example, you can create an alias to represent the first part of a command, and then type the rest part of the command.

The mode of the command represented by the alias is the command mode existing in the current system. In the global configuration mode, you can use the **alias ?** command to list all the modes under which you can configure alias for commands.

```
Ruijie(config)# alias ?
aaa-gs          AAA server group mode
acl             acl configure mode
bgp             Configure bgp Protocol
config         globle configure mode
.....
```

The alias also has its help information that is displayed after * in the following format:

```
*command-alias=original-command
```

For example, in the privileged EXEC mode, the default alias s stands for show. You can enter s? to query the key words beginning with s and the help information of the alias.

```
Ruijie#s?
```

```
*s=show show start-chat start-terminal-service
```

If an alias represents more than one word, the command will be displayed in brackets. For example, if you set sv stand for show version in the privileged EXEC mode, then:

```
Ruijie#s?
```

```
*s=show *sv="show version" show start-chat
start-terminal-service
```

The alias must begin with the first letter of the command. The first letter of the command cannot be a space. The space before the command cannot be used as a valid alias.

```
Ruijie# s?
```

```
show start-chat start-terminal-service
```

The command alias also has its help information. For example, if the alias ia represents ip address in the interface configuration mode, then:

```
Ruijie(config-if)#ia ?
```

```
  A.B.C.D IP address
```

```
  dhcp   IP Address via DHCP
```

```
Ruijie(config-if)# ip address
```

The above help information lists the parameters of **ip address** and shows the actual command name. You must enter an entire alias; otherwise it cannot be recognized.

Use the **show aliases** command to show the aliases setting in the system.

Configuration Examples The following example uses def-route to represent the default route setting of ip route 0.0.0.0 0.0.0.0 192.168.1.1 in the global configuration mode:

```
Ruijie# configure terminal
```

```
Ruijie(config)# alias config def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

```
Ruijie(config)#def-route?
```

```
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
```

```
Ruijie(config)# end
```

```
Ruijie# show aliases config
```

```
globe configure mode alias:
```

```
def-route          ip route 0.0.0.0 0.0.0.0
```

```
192.168.1.1
```

Related Commands

Command	Description
show aliases	Displays the aliases settings.

Platform Description N/A

1.2 privilege

Use this command to attribute the execution rights of a command to a command level in global configuration mode. Use the **no** form of this command to restore the default setting.

privilege *mode* [**all**] [**level** *level* | **reset**] *command-string*

no privilege *mode* [**all**] [**level** *level*] *command-string*

Parameter Description	Parameter	Description
	<i>mode</i>	CLI mode of the command to which the execution rights are attributed.
	all	Command alias
	level <i>level</i>	Specifies the execution right levels (0–15) of a command or sub-commands
	reset	Restores the command execution rights to its default level
	<i>command-string:</i>	Command string to be authorized

Defaults N/A

Command Mode Global configuration mode.

Usage Guide The following table lists some key words that can be authorized by the **privilege** command in CLI mode. The number of command modes that can be authorized may vary with different devices. In the global configuration mode, you can use the **privilege ?** command to list all CLI command modes that can be authorized.

Mode	Descriptor
config	Global configuration mode.
exec	Privileged EXEC mode
interface	Interface configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
keychain	KeyChain configuration mode
keychain-key	KeyChain-key configuration mode

Configuration Examples The following example sets the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

```
Ruijie(config)#privilege exec level 1 reload
```

You can access the CLI window as level-1 user to use the **reload** command:

```
Ruijie>reload ?
```

```
LINE Reason for reload
```

<cr> You can use the key word **all** to attribute all sub-commands of reload to level-1 users:

```
Ruijie(config)# privilege exec all level 1 reload
```

After the above setting, you can access the CLI window as level-1 user to use all sub commands of the **reload** command:

```
Ruijie>reload ?
LINE      Reason for reload
at                reload at a specific time/date
cancel           cancel pending reload scheme
in              reload after a time interval
<cr>
```

Related Commands

Command	Description
enable secret	Sets the CLI-level password.

Platform N/A.
Description

1.3 show aliases

Use this command to show all the command aliases or aliases in special command modes.

show aliases [*mode*]

Parameter Description

Parameter	Description
<i>mode</i>	Mode of the command represented by the alias.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide This command displays the configuration of all aliases if no command mode is input.

Configuration The following example displays the command alias in privileged EXEC mode:

Examples

```
Ruijie#show aliases exec
exec mode alias:
h                help
p                ping
s                show
u                undebug
un              undebug
```

Related Commands

Command	Description
alias	Sets a command alias.

Platform N/A.
Description

2 Basic Configuration Management Commands

2.1 <1-99>

Use this command to restore the suspended Telnet Client session.

<1-99>

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode User EXEC mode

Usage Guide This command is used to restore the suspended Telnet Client session. Hot keys (ctrl+shift+6 x) are used to exit the Telnet Client session creation. The **<1-99>** command is used to restore the session. If the session is created, you can use the **show session** command to display the session.

Configuration Examples The following example restores the suspended Telnet Client session.

```
Ruijie# 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.2 banner exec

Use this command to configure a message to welcome the user entering user EXEC mode through the line. Use the **no** form of this command to restore the default setting.

banner exec c message c

no banner exec

Parameter Description	Parameter	Description
	c	Separator of the message. Delimiters are not allowed in the message.

<i>message</i>	Contents of the message.
----------------	--------------------------

Defaults N/A

Command Global configuration mode

Mode

Usage Guide This command is used to configure the welcome message. The system discards all the characters next to the terminating symbol.

When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the EXEC message or the incoming message is displayed. If it's a reverse Telnet session, the incoming message is displayed. Otherwise, the EXEC message is displayed.

The messages are for all lines. If you want to disable display the EXEC message on a specific line, configure the **no exec-banner** command on the line.

Configuration The following example configures a welcome message.

Examples Ruijie(config)# banner exec \$ Welcome \$

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.3 banner incoming

Use this command to configure a prompt message for reverse Telnet session. Use the **no** form of this command to remove the setting.

banner incoming *c message c*

no banner incoming

**Parameter
Description**

Parameter	Description
<i>c</i>	Separator of the message. Delimiters are not allowed in the message.
<i>message</i>	Contents of the message.

Defaults N/A

Command Global configuration mode

Mode

Usage Guide This command is used to configure a prompt message. The system discards all the characters next to the terminating symbol.

When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the welcome message or the prompt message is displayed. If it's a reverse Telnet session, the prompt message is displayed. Otherwise, the welcome message is displayed.

Configuration The following example configures a prompt message for reverse Telnet session.

Examples

```
Ruijie(config)# banner incoming $ Welcome $
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.4 banner login

Use this command to configure a login banner. Use **no** form of this command to r remove the setting.

banner login c message c

no banner login

**Parameter
Description**

Parameter	Description
<i>c</i>	Separator of the message contained in the login banner. Delimiters are not allowed in the MOTD.
<i>message</i>	Contents of the login banner

Defaults

N/A

**Command
Mode**

Global configuration mode

Usage Guide

This command sets the login banner message, which is displayed at login. The system discards all the characters next to the terminating symbol.

Configuration The following example configures a login banner.

Examples

```
Ruijie(config)# banner login $ enter your password $
```

**Related
Commands**

Command	Description
N/A	N/A

Platform
Description N/A

2.5 banner motd

Use this command to set the Message-of-the-Day (MOTD) . Use the **no** form of this command to remove the setting.

banner [motd] c message c

no banner [motd]

Parameter Description	Parameter	Description
	<i>c</i>	Separator of the MOTD. Delimiters are not allowed in the MOTD.
	<i>message</i>	Contents of an MOTD

Defaults N/A

Command Global configuration mode
Mode

Usage Guide This command sets the MOTD, which is displayed at login. The letters that follow the separator will be discarded.

Configuration The following example configures the MOTD.

Examples Ruijie(config)# **banner motd** \$ *hello,world* \$

Related Commands	Command	Description
	N/A	N/A

Platform
Description N/A

2.6 banner prompt-timeout

Use this command to configure the prompt-timeout message to notify timeout. Use the **no** form of this command to remove the setting.

banner prompt-timeout c message c

no banner prompt-timeout

Parameter Description	Parameter	Description
	<i>c</i>	Separator of the message. Delimiters are not allowed in the

	message.
<i>message</i>	Contents of the message.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The system discards all the characters next to the terminating symbol.
When authentication times out, the banner prompt-timeout message is displayed.

Configuration The following example configures the prompt-timeout message to notify timeout.

Examples Ruijie(config)# banner exec \$ authentication timeout \$

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.7 banner slip-ppp

Use this command to configure the slip-ppp message for the SLIP/PPP session. Use the **no** form of this command to remove the setting.

banner slip-ppp c message c

no banner slip-pp

Parameter Description	Parameter	Description
	<i>c</i>	
<i>message</i>		Contents of the message.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure the slip-ppp message for the SLIP/PPP session. The system discards all the characters next to the terminating symbol.
When the SLIP/PPP session is created, the slip-ppp message is displayed on the corresponding terminal.

Configuration The following example configures the banner slip-ppp message for the SLIP/PPP session.

Examples

```
Ruijie(config)# banner slip-ppp $ Welcome $
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.8 boot config

Use this command to modify the path for saving startup configurations and the corresponding file name.

boot config { flash:filename | usb0:filename }

no boot config

**Parameter
Description**

Parameter	Description
flash	Saves the startup configuration file in the extensible Flash.
usb0	Saves the startup configuration file in USB0 device. The device must have a USB interface into which a USB device is inserted.




Defaults

By default, startup configuration file of a device is saved in **Flash:/config.text**

**Command
Mode**

Privileged EXEC mode

Usage Guide

-  The startup configuration file name follows a slash "/", for example, **Flash:/ruijie.text** and **Usb0:/ruijie.text**.
-  The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the **write** command. Take **Flash:/ruijie/ruijie.text** and **Usb0:/ruijie/ruijie.text** as examples, where the **Flash:/ruijie** and **Usb0:/ruijie** folders must exist. In master-slave mode, all device paths are required.
-  To save the startup configuration file to a USB flash drive, the device must provide a USB interface with a USB flash drive inserted. Otherwise, configurations cannot be saved by using the **write** command. In master-slave mode, all devices must have USB flash drives connected.

Configuration The following example sets the startup configuration file path to flash:/ruijie.text..

Examples

```
Ruijie(config)#boot config flash:/ruijie.text
```

Related Commands	Command	Description
	N/A	N/A

Platform
Description N/A

2.9 checkpoint

Use this command to create a checkpoint. Use the **no** form of this command to remove the setting.

checkpoint [*cp-name*] [**description** *description*]

no checkpoint *cp-name*

Parameter Description	Parameter	Description
		<i>cp-name</i>
	description <i>description</i>	(Optional) specifies the checkpoint description, in the range from 1 to 80 characters.

Defaults N/A

Command Privileged EXEC mode
Mode

Usage Guide If you do not name a checkpoint, the system specifies a name automatically. The description is null by default. When a checkpoint is created, the copy of the current configuration is saved.

Configuration The following example creates a checkpoint with a default name.

Examples

```
Ruijie# checkpoint
...
user-checkpoint-1 created Successfully
```

Related Commands	Command	Description
	N/A	N/A

Platform
Description N/A

2.10 clear checkpoint database

Use this command to clear the checkpoint statistics.

clear checkpoint database

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears the checkpoint statistics.

Examples Ruijie# clear checkpoint database

Related Commands	Command	Description
		N/A

Platform Description N/A

2.11 configure

Use this command to enter global configuration mode.

configure [terminal]

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example enters global configuration mode.

Examples Ruijie# configure
Ruijie(config)#

Related	Command	Description

Commands		
	N/A	N/A

Platform Description N/A

2.12 disable

Use this command to switch from privileged EXEC mode to user EXEC mode or lower the privilege level.

disable [*privilege-level*]

Parameter Description	Parameter	Description
	privilege-level	Privilege level

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to switch to user EXEC mode from privileged EXEC mode. If a new privilege level is added, the current privilege level will be lowered.

 The privilege level that follows the **disable** command must be lower than the current level.

Configuration Examples The following example lowers the current privilege level of the device to level 10.

```
Ruijie# disable 10
```

Related Commands	Command	Description
	enable	Moves from user EXEC mode enter to privileged EXEC mode or reaches a higher level of authority.

Platform Description N/A

2.13 disconnect

Use this command to disconnect the Telnet Client session.

disconnect *session-id*

Parameter Description	Parameter	Description
	<i>session-id</i>	Telnet Client session ID.
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	This command is used to disconnect the Telnet Client session by setting the session ID.	
Configuration Examples	The following example disconnects the Telnet Client session by setting the session ID.	
Examples	<pre>Ruijie# disconnect 1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.14 do telnet

Use this command to login to Telnet server.

```
do telnet [ oob ] host [ port ] [ /source { ip A.B.C.D | ipv6 X:X:X::X | interface interface-name } ]
[ /vrf vrf-name ] [ via mgmt-name ]
```

Parameter Description	Parameter	Description
	oob	Connects to Telnet server through oob channel. This parameter is available only when the device has a MGMT port.
	<i>host</i>	IPv4, IPv6 or host name of Telnet server.
	<i>port</i>	Configures TCP port ID. The default is 23.
	/source	Specifies source IP or source port for Telnet client.
	ip <i>A.B.C.D</i>	Specifies source IPv4 address for Telnet client.
	ipv6 <i>X:X:X::X</i>	Specifies source IPv6 address for Telnet client.
	interface <i>interface-name</i>	Specifies source port for Telnet client.
	/vrf <i>vrf-name</i>	Specifies VRF table.
	via <i>mgmt-name</i>	Specifies MGMT table.
Defaults	N/A	

Command Mode User EXEC mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example configures destination IPv4 address 192.168.1.1, uses default port ID, and specifies source port Gi 0/1 and VRF table vpn1.

```
Ruijie(config)# do telnet 192.168.1.1 /source interface gigabitEthernet 0/1 /vrf vpn1
```

The following example configures destination IPv6 address 2AAA:BBBB::CCCC.

```
Ruijie(config)# do telnet 2AAA:BBBB::CCCC
```

The following example configures destination IPv4 address 192.168.1.1 and specifies MGMT port Mgmt 0.

```
Ruijie(config)# do telnet oob 192.168.1.1 via mgmt 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.15 enable

Use this command to enter privileged EXEC mode.

enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode N/A

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform
Description

N/A

2.16 enable password

Use this command to configure passwords for different privilege levels. Use the **no** form of this command to restore the default setting.

enable password [level *level*] { password | [0 | 7] *encrypted-password* }

no enable password [level *level*]

Parameter
Description

Parameter	Description
password	Password for the user to enter the EXEC configuration layer
level	User's level.
0 7	Password encryption type, "0" for no encryption, "7" for simple encryption (Optional) Ruijie's private algorithm will be used for password encryption. If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted by a Ruijie device.
encrypted-password	Password text.

Defaults

N/A

Command
Mode


Global configuration mode

Usage Guide

No encryption is required in general. The encryption type must be specified for copying and pasting a encrypted password for the device.

A valid password is defined as follows:

- Consists of 1-26 upper/lower case letters and numbers
- Leading spaces are allowed but usually ignored. Spaces in between or at the end are regarded as part of the password.

 If an encryption type is specified and a plaintext password is entered, you cannot enter privileged EXEC mode. A lost password that has been encrypted using any method cannot be restored. In this case, you can only reconfigure the device password.

Configuration The following example configures the password as **pw10**.

Examples

```
Ruijie(config)# enable password pw10
```

Related

Command	Description
---------	-------------

Commands	
enable secret	Sets the security password

Platform

N/A

Description**enable secret** Sets the security password

2.17 enable secret

Use this command to configure a security password for different privilege levels. Use the **no** form of this command to restore the default setting.

enable secret [level *level*] { *secret* | [0 | 5] *encrypted-secret* }

no enable secret [level *level*]

Parameter Description	Parameter	Description
	secret	Password for the user to enter the EXEC configuration layer
	level	User's level.
	0 5	Password encryption type, "0" for no encryption, "5" for security encryption
	encrypted-password	Password text

Defaults

N/A

Command

Global configuration mode

Mode**Usage Guide**

A password comes under two categories: "password" and "security". "Password" indicates a simple password, which can be set only for level 15. "Security" means a security password, which can be set for levels 0-15. If both types of passwords coexist in the system, no "password" type is allowed. If a "password" type password is set for a level other than 15, the system gives an alert and the password is automatically converted into a "security" password. If a "password" type password is set for level 15 and the same as a "security" password, an alert is given. The password must be encrypted, with simple encryption for "password" type passwords and security encryption for "security" type passwords.

Configuration

The following example configures the security password as **pw10**.

Examples

```
Ruijie(config)# enable secret 0 pw10
```

Related**Commands**

Command	Description
enable password	Sets passwords for different privilege levels.

Platform
Description

N/A

2.18 enable service

Use this command to enable or disable a specified service such as **SSH Server/Telnet Server/Web Server/SNMP Agent**.

enable service { **ssh-sesrver** | **telnet-server** | **web-server** [**http** | **https** | **all**] | **snmp-agent** }

Parameter
Description

Parameter	Description
ssh-server	Enables SSH Server. IPv4 and IPv6 services are enabled at the same time.
telnet-server	Enables Telnet Server. IPv4 and IPv6 services are enabled at the same time.
web-server [http https all]	Enables HTTP Server. IPv4 and IPv6 services are enabled at the same time.
snmp-agent	Enables SNMP Agent. IPv4 and IPv6 services are enabled at the same time.

Defaults


N/A

Command
Mode

Global configuration mode

Usage Guide

Use this command to enable or disable a specified service. Use the **no enable service** command to disable the specified service.

 The **enable service web-server** command is followed by three optional keywords: [http | https | all]. If the command is followed by no keyword or by **all**, the command enables http and https services. Followed by **http**, the command enables http service only. Followed by **https**, the command enables https service only.

Configuration The following example enables the SSH Server.

Examples

```
Ruijie(Config)# enable service ssh-sesrver
```

Related
Commands

Command	Description
show service	Displays the service status in the current system.

Platform
Description

N/A

2.19 end

Use this command to return to privileged EXEC mode.

end

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode All modes except privileged EXEC mode

Usage Guide N/A

Configuration The following example returns to privileged EXEC mode.

Examples

```
Ruijie#con
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#line vty 0
Ruijie(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.20 exec-banner

Use this command to enable display of the EXEC message on a specific line. Use the **no** form of this command to restore the default setting.

exec-banner

no exec-banner

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The EXEC message is displayed on all lines by default.

Command LINE configuration mode
Mode

Usage Guide After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.

i This command does not work for the banner incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

Configuration The following example disables display of the EXEC message on line VTY 1.

Examples

```
Ruijie(config)# line vty 1
Ruijie(config-line)no exec-banner
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.21 exec-timeout

Use this command to configure connection timeout for this device in LINE mode. Use the **no** form of this command to restore the default setting and the connection never expires.

exec-timeout *minutes* [*seconds*]

no exec-timeout

**Parameter
Description**

Parameter	Description
<i>minutes</i>	Timeout in minutes.
seconds	(Optional) Timeout in minutes

Defaults The default is 10 minutes.

**Command
Mode** Line configuration mode

Usage Guide If there is no input or output for this connection within a specified time, this connection will expire, and this LINE will be restored to the free status.

Configuration The following example sets the connection timeout to 5'30".

Examples Ruijie(config-line)#~~exec-timeout~~ 5 30

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.22 exit

Use this command to return to the upper configuration mode.

exit

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

N/A

**Command
Mode**

All configuration modes

Usage Guide

N/A

Configuration The following example returns to the upper configuration mode.

Examples

```
Ruijie#con
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#line vty 0
Ruijie(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#con
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#line vty 0
Ruijie(config-line)#exit
Ruijie(config)#exit
*May 20 09:51:48: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#exit

Press RETURN to get started
```

**Related
Commands**

Command	Description
N/A	N/A

Platform
Description

N/A

2.23 help

Use this command to display the help information.

help

Parameter
Description

Parameter	Description
N/A	N/A

Defaults Any mode

Command
Mode

Usage Guide This command is used to display brief information about the help system. You can use "?" to display all commands or a specified command with its parameters.

Configuration The following example displays brief information about the help system.

Examples

```
Ruijie#help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

The following example displays all available commands in interface configuration mode.

```
Ruijie(config-if-GigabitEthernet 0/0)#?
```

Interface configuration commands:

```
arp          ARP interface subcommands
bandwidth    Set bandwidth informational parameter
carrier-delay Specify delay for interface transitions
dampening    Enable event dampening
default      Set a command to its defaults
description  Interface specific description
lldp         Exec data link detection command
```

duplex	Configure duplex operation
efm	Config efm for an interface
end	Exit from interface configuration mode
exit	Exit from interface configuration mode
expert	Expert extended ACL
flowcontrol	Set the flow-control value for an interface
full-duplex	Force full duplex operation
global	Global ACL
gvrp	GVRP configure command
half-duplex	Force half duplex operation
help	Description of the interactive help system
ip	Interface Internet Protocol config commands
ipv6	Internet Protocol Version 6
isis	Intermediate System - Intermediate System (IS-IS)
l2	Config L2 attribute
label-switching	Enable interface process mpls packet
lacp	LACP interface subcommands
lldp	Link Layer Discovery Protocol
load-interval	Specify interval for load calculation for an interface
mac	Mac extended ACL
mac-address	Set mac-address
mpls	Multi-Protocol Label Switching
mtu	Set the interface Maximum Transmission Unit (MTU)
no	Negate a command or set its defaults
ntp	Configure NTP
port-group	Aggregateport/port bundling configuration
redirect	Redirect packets
rmon	Rmon command
security	Configure the Security
show	Show running system information
shutdown	Shutdown the selected interface
snmp	Modify SNMP interface parameters
speed	Configure speed operation
switchport	Set switching mode characteristics
vrf	Multi-af VPN Routing/Forwarding parameters on the interface
vrrp	VRRP interface subcommands
xconnect	Xconnect commands

The following example displays the parameters of a specified command.

```
Ruijie(config)#access-list 1 permit ?
A.B.C.D Source address
any Any source host
host A single source host
```

Related**Command****Description**

Commands		
	N/A	N/A

Platform
Description N/A

2.24 hostname

Use this command to specify or modify the hostname of a device.

hostname *name*

Parameter Description	Parameter	Description
	<i>name</i>	Device hostname, string, number or hyphen, up to 63 characters.

Defaults The default is Ruijie.

Command Global configuration mode
Mode

Usage Guide This hostname is mainly used to identify the device and is taken as the username for the local device during dialup and CHAP authentication.

Configuration The following example configures the hostname of the device as BeiJingAgenda.

Examples

```
Ruijie(config)# hostname BeiJingAgenda
BeiJingAgenda(config)#
```

Related Commands	Command	Description
	N/A	N/A

Platform
Description N/A

2.25 ip telnet source-interface

Use this command to configure the IP address of an interface as the source address for Telnet connection.

ip telnet source-interface *interface-name*

Parameter Description	Parameter	Description
	<i>interface-name</i>	Configures the IP address of the interface as the source address for

	Telnet connection.
--	--------------------

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to specify the IP address of an interface as the source address for global Telnet connection. When using the telnet command to log in a Telnet server, apply the global setting if no source interface or source address is specified. Use the **no ip telnet source-interface** command to restore it to the default setting.

Configuration Examples The following example configures the IP address of the *Loopback1* interface as the source address for global Telnet connection.

```
Ruijie(Config)# ip telnet source-interface Loopback 1
```

Related Commands

Command	Description
telnet	Logs in a Telnet server.

Platform Description N/A

2.26 lock

Use this command to set a temporary password for the terminal.

lock

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can lock the terminal interface and maintain the session continuity to prevent access to the interface by setting a temporary password. Take the following steps to lock the terminal interface:

- Enter the **lock** command, and the system will prompt you for a password:
- Enter the password, which can be any character string. The system will prompt you to confirm the password, clear the screen, and display the "Locked" information.
- To access the terminal, enter the preset temporary password.
- To lock the terminal, run the **lockable** command in line configuration mode and enable terminal

locking in the corresponding line.

Configuration The following example locks a terminal interface.

```
Examples
Ruijie(config-line)# lockable
Ruijie(config-line)# end
Ruijie# lock
Password: <password>
Again: <password>
Locked
Password: <password>
Ruijie#
```

**Related
Commands**

Command	Description
lockable	Supports terminal locking in the line.

**Platform
Description** N/A

2.27 lockable

Use this command to support the **lock** command at the terminal. Use the **no** form of this command to restore the default setting.

lockable
no lockable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

Command This function is disabled by default.

Mode

Usage Guide This command is used to lock a terminal interface in the corresponding line. To lock the terminal, run the lock command in EXEC mode.

Configuration The following example enables terminal locking at the console port and locks the console.

```
Examples
Ruijie(config)# line console 0
Ruijie(config-line)# lockable
Ruijie(config-line)# end
Ruijie# lock
Password: <password>
```

```
Again: <password>
Locked
Password: <password>
```

**Related
Commands**

Command	Description
lock	Locks the terminal.

**Platform
Description**

N/A

2.28 login

Use this command to enable simple login password authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

login**no login****Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

N/A

**Command
Mode**

Line configuration mode

Usage Guide

If the AAA security server is inactive, this command enables simple password authentication at login. The password is configured for a VTY or console interface.

Configuration

The following example sets a login password authentication on VTY..

Examples

```
Ruijie(config)# no aaa new-model
Ruijie(config)# line vty 0
Ruijie(config-line)# password 0 normatest
Ruijie(config-line)# login
```

**Related
Commands**

Command	Description
password	Configures the line login password

**Platform
Description**

N/A

2.29 login authentication

If the AAA is enabled, login authentication must be performed on the AAA server. Use this command to associate login authentication method list. Use the **no** form of this command to restore the default setting.

login authentication { **default** | *list-name* }

no login authentication { **default** | *list-name* }

Parameter Description

Parameter	Description
default	Name of the default authentication method list
<i>list-name</i>	Name of the method list

Defaults N/A

Command Mode Line configuration mode

Usage Guide If the AAA security server is active, this command is used for login authentication using the specified method list.

Configuration Examples The following example associates the method list on VTY and perform login authentication on a radius server.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authentication login default radius
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication login	Configures the login authentication method list.

Platform Description N/A

2.30 login local

Use this command to enable local user authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

login local

no login local

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	If the AAA security server is inactive, this command is used for local user login authentication. The user is allowed to use the username command.	
Configuration	The following example sets local user authentication on VTY.	
Examples	<pre>Ruijie(config)# no aaa new-model Ruijie(config)# username test password 0 test Ruijie(config)# line vty 0 Ruijie(config-line)# login local</pre>	
Related Commands	Command	Description
	username	Configures local user information.
Platform Description	N/A	

2.31 login privilege log

Use this command to log privilege change. Use the **no** form of this command to restore the default setting.

login privilege log

no login privilege log

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This command is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration	The following example enables the function of logging privilege change.	

Examples

```
Ruijie(config)# login privilege log
```

The following example displays the log of privilege change failure.

```
Ruijie>enable 10
```

```
Password:
```

```
Password:
```

```
Password:
```

```
% Access denied
```

```
Ruijie>
```

```
*Sep 10 11:34:19: %SYS-5-PRIV_AUTH_FAIL: Authentication to
privilege level 10 from console failed
```

The following example displays the log of privilege change success.

```
Ruijie>enable 10
```

```
Password:
```

```
Ruijie#
```

```
*Sep 10 11:34:20: %SYS-5-PRIV_AUTH_SUCCESS: Authentication to
privilege level 10 from console success
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.32 motd-banner

Use this command to enable display of the MOTD message on a specified line. Use the **no** form of this command to restore the default setting.

motd-banner

no motd-banner

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

The MOTD message is displayed on all lines by default.

**Command
Mode**

Line configuration mode

Usage Guide

After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD

messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.

- i** This command does not work for the incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

Configuration The following example disables display of the MOTD message on VTY 1.

Examples

```
Ruijie(config)# line vty 1
Ruijie(config-line)no motd-banner
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

2.33 password

Use this command to configure a password for line login, run the **password** command. Use the **no** form of this command to restore the default setting.

password { *password* | [**0** | **7**] *encrypted-password* }

no password

**Parameter
Description**

Parameter	Description
<i>password</i>	Password for remote line login
0 7	Password encryption type, "0" for no encryption, "7" for simple encryption (Optional) Ruijie's private algorithm will be used for password encryption. If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted by a Ruijie device.
<i>encrypted-password</i>	Password text

Defaults

N/A

**Command
Mode**

Line configuration mode

Usage Guide

This command is used to configure a authentication password for remote line login.

Configuration The following example configures the line login password as "red".

Examples

```
Ruijie(config)# line vty 0
```

```
Ruijie(config-line)# password red
```

**Related
Commands**

Command	Description
login	Moves from user EXEC mode to privileged EXEC mode or enables a higher level of authority.

**Platform
Description**

N/A

2.34 prompt

Use this command to set the **prompt** command. Use the **no** form of this command to restore the default setting.

prompt string

**Parameter
Description**

Parameter	Description
string	Character string of the prompt command, containing up to 32 letters.

Defaults

N/A

**Command
Mode**

Global configuration mode

Usage Guide

If no prompt string is configured, the system name applies and varies with the system name. The **prompt** command is valid only in EXEC mode.

Configuration

The following example sets the prompt string to rgos.

Examples

```
Ruijie(config)# prompt rgos
Ruijie(config)# end
RGOS
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.35 rollback

Use this command to roll back the checkpoint configuration.




rollback running-config checkpoint *cp-name* [**display-differences** | **ignore-results**]

Parameter Description	Parameter	Description
	<i>cp-name</i>	Specifies the checkpoint name, in the range from 1 to 80 characters.
	display-differences	Displays configuration difference after the rollback is complete. The configuration difference is displayed by default.
	ignore-results	Ignores results after the rollback is complete. The configuration difference is not displayed.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

-  Only one user is allowed to create a checkpoint and roll back configuration on the device.
-  If an "Increased configuration" message is displayed after the rollback is complete, it indicates that some command does not support reverse operation or the reverse operation fails. It is recommended to see the *Command Reference* for details and execute the reversion of the command manually.
-  If a "Decreased configuration" message is displayed after the rollback is complete, it indicates that it fails to execute some command during the rollback. It is recommended to see the *Command Reference* for details and execute the command manually.

Configuration The following example rolls back the configuration of checkpoint user-1.

Examples

```
Ruijie# rollback running-config checkpoint user-checkpoint-1 ignore-results
...
Rollback configuration successfully.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.36 secret

Use this command to set a password encrypted by irreversible MD5 for line login. Use the **no** form of this command to restore the default setting.

secret { [**0**] *password* | **5** *encrypted-secret* }


no secret

Parameter Description	Parameter	Description
	0	(Optional) sets the plaintext password text and encrypts it with irreversible MD5 after configuration.
	<i>password</i>	Sets the password plaintext, a string ranging from 1 to 25 characters.
	5 <i>encrypted-secret</i>	Sets the password text encrypted by irreversible MD5 and saves it as the encrypted password after configuration.

Defaults N/A

Command mode Line configuration mode

Usage Guide This command is used to set a password encrypted by irreversible MD5 that is authenticated by a remote user through line login.

 If the specified encryption type is 5, the logical length of the cipher text to be entered must be 24 and the 1st, 3rd and 8th characters of the password text must be \$.

In general, the encryption type does not need to be specified as 5 except when the encrypted password is copied and pasted.

Line mode allows configuration of both “password” and “secret” types passwords at the same time. When the two passwords are the same, the system will send alert notification but the configuration will be permitted. When the system is configured with the two passwords, if the user enters a password that does not match the “secret” type password, it will not continue to match the “password” type password and login fails, enhancing security for the system password.

Configuration The following example sets the password encrypted by irreversible MD5 for line login to vty0.

Examples

```
Ruijie(config)# line vty 0
```

```
Ruijie(config-line)# secret vty0
```

The following displays the encryption outcome by running the **show** command.

```
secret 5 $1$X834$wvx6y794uAD8svzD
```

Related Commands	Command	Description
	login	Sets simple password authentication on the interface as the login authentication mode

Platform N/A
Description

2.37 session

Use this command to connect to the management module or the service module through session in VSU master-slave environment (card-type device).

session { **master** | [**device** *device-number*] **slot** { **m1** | **m2** | *slot-number* } }

Use this command to connect to another device in VSU multiple-device environment (box-type device).

session { **master** | **device** *device-number* }

Parameter Description	Parameter	Description
	master	Configures the slave host to connect with the master host or the slave management module with the master management module.
	device <i>device-number</i>	Sets the device number.
	slot { m1 m2 }	Sets the management module to either m1 or m2.
	slot <i>slot-number</i>	Sets the device slot ID for service module connection.

Defaults N/A

Command Mode User EXEC mode

Usage Guide N/A

Configuration Examples The following example configures the slave host to connect with the master host in VSU environment.

```
Ruijie# session master
```

The following example connects to device1 through session in VSU multiple-device environment (box-type device).

```
Ruijie# session device 1
```

The following example connects to management module m1 of device1 through session in VSU master-slave environment (card-type device).

```
Ruijie# session device 1 slot m1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.38 session-timeout

Use this command to configure the session timeout for a remote terminal. Use the **no** form of this command to restore the default setting and the session never expires.

session-timeout *minutes* [**output**]

no session-timeout

Parameter Description	Parameter	Description
	<i>minutes</i>	Timeout in minutes.
	output	Regards data output as the input to determine whether the session expires.

Defaults The default timeout is 0.

Command Mode LINE configuration mode

Usage Guide If no input or output in current LINE mode is found on the remote terminal for the session within a specified time, this connection will expire, and this LINE will be restored to the free status.

Configuration Examples The following example specifies the timeout as 5 minutes.

```
Ruijie(config-line)#exec-timeout 5 output
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.39 show boot config

Use this command to display the path and file name of the startup configuration.

show boot config

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode**Usage Guide** N/A**Configuration** The following example displays the path and file name of the startup configuration.**Examples**

```
Ruijie#show boot config
Boot config file: [flash:/ruijie.text]
```

**Related
Commands**

Command	Description
N/A	N/A

Platform**Description**

N/A

2.40 show checkpoint

Use this command to display information of a specified checkpoint or summary information of all checkpoints.

show checkpoint { *cp-name* [**all**] | **summary** }

**Parameter
Description**

Parameter	Description
<i>cp-name</i>	Specifies the checkpoint name, in the range from 1 to 80 characters.
all	(Optional) Displays detailed information of all checkpoints.
summary	Displays summary information of all checkpoints.

Defaults

N/A

Command

Privileged EXEC mode

Mode**Usage Guide**

N/A

**Configuratio
n Examples**

The following example displays the summary information of all checkpoints.

```
Ruijie# show checkpoint summary
User Checkpoint Summary
-----
----
1) user-checkpoint-1:
Created at 16:08:30 30 May 2014
Size is 3,566 bytes
```

Description: None	
Field	Description
user-checkpoint-1	Checkpoint name.
Created at 16:08:30 30 May 2014	Checkpoint creation time.
Size is 3,566 bytes	Size of configuration copy.
Description: None	Checkpoint description.

Related Commands	Command	Description
	N/A	N/A

Platform
Description N/A

2.41 show debugging

Use this command to display debugging state.

show debugging

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays debugging state.

```
Ruijie#show debugging

debug fw-group detect intf-state
```

Related Commands	Command	Description
	N/A	N/A

Platform
Description N/A

2.42 show line

Use this command to display the configuration of a line.

show line { **console** *line-num* | **vt**y *line-num* | *line-num* }

Parameter Description	Parameter	Description
	console	Display s the configuration of a console line.
	aux	Checks configuration information relating to the aux line.
	vt y	Display s the configuration of a vty line.
	<i>line-num</i>	Number of the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the configuration of a line.

Configuration Examples The following example displays the configuration of a console port.

```
Ruijie# show line console 0
CON   Type    speed  Overruns
* 0   CON     9600  45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape Disconnect Activation
                ^^x   none      ^M
Timeouts:      Idle EXEC   Idle Session
                never    never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output: 395756 bytes
Data overflow: 27697 bytes
stop rx interrupt: 0 times
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.43 show reload

Use this command to display the system restart settings.

show reload

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the restart settings of the system.

Configuration The following example displays the restart settings of the system.

Examples

```
Ruijie# show reload
Reload scheduled in 595 seconds.
At 2003-12-29 11:37:42
Reload reason: test.
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.44 show running-config

Use this command to display how the current device system is configured..

show running-config

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration N/A

Examples

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.45 show service

Use this command to display the service status.

show service

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays whether the service is enabled or disabled.

Examples

```
Ruijie# show service
web-server : disabled
web-server(https): disabled
snmp-agent : enabled
ssh-server : enabled
telnet-server : disabled
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.46 show sessions

Use this command to display the Telnet Client session information.

show sessions

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode User EXEC mode

Usage Guide Telnet Client session information includes the VTY number and the server IP address.

Configuration The following example displays the Telnet Client session information.

Examples

```
Ruijie#show sessions
Conn  Address
*1    127.0.0.1
*2    192.168.21.122
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.47 show startup-config

Use this command to display the device configuration stored in the Non Volatile Random Access Memory (NVRAM).

show startup-config

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The device configuration stored in the NVRAM is executed while the device is starting.

On a device that does not support **boot config**, **startup-config** is contained in the default configuration file **/config.text** in the built-in flash memory.

On a device that supports **boot config**, configure **startup-config** as follows:

If you have specified a boot configuration file using the **boot config** command and the file exists, **startup-config** is stored in the specified configuration file.

If the boot configuration file you have specified using the **boot config** command does not exist or you have not specified a boot configuration file using the command, **startup-config** is contained in **/config.text** in the built-in flash memory.

Configuration N/A

Examples

Related Commands	Command	Description
		boot config

Platform Description N/A

2.48 show this

Use this command to display effective configuration in the current mode.

show this

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode All modes.

Usage Guide The configuration in the following range modes cannot be displayed. If the **show this** command is run, the outcome is NULL.

1. Use the **line first-line last-line** command to configure lines in a continuous group and enter LINE configuration mode.
2. Use the **vlan range** command to configure VLANs and enter vlan range configuration mode.
3. Use the **interface range** command to configure interfaces and enter interface range configuration mode.

Configuration Use this command to display effective configuration on interface fastEthernet 0/1.

Examples

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)#show this
Building configuration...
!
spanning-tree link-type point-to-point
spanning-tree mst 0 port-priority 0
!
end
Ruijie (config-if-FastEthernet 0/1)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.49 speed

Use this command to set the speed at which the terminal transmits packets. Use the **no** form of this command to restore the default setting.

speed *speed*
no speed

Parameter Description	Parameter	Description
	<i>speed</i>	

Defaults The default is 9600.

Command Mode Global configuration mode

Usage Guide This command is used to set the speed at which the terminal transmits packets.

Configuration Examples The following example sets the rate of the serial port to 57600 bps.

```
Ruijie(config)# line console 0
Ruijie(config-line)# speed 57600
```

Related Commands	Command	Description

N/A	N/A
-----	-----

Platform
Description

N/A

2.50 telnet

Use this command to log in a server that supports telnet connection.

telnet *host* [*port*] [/**source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X* | **interface** *interface-name* }] [/**vrf** *vrf-name*] [**via** *mgmt-name*]

Parameter
Description

Parameter	Description
Host	The IP address of the host or host name you want to log in.
Port	Selects the TCP port number for login, 23 by default.
/source	Specifies the source IP address or source interface used by the Telnet client.
ip <i>A.B.C.D</i>	Specifies the source IPv4 address used by the Telnet client.
ipv6 <i>X:X:X:X</i>	Specifies the source IPv6 address used by the Telnet client.
interface <i>interface-name</i>	Specifies the source interface used by the Telnet client.
/vrf <i>vrf-name</i>	Specifies the VRF routing table you want to query.
via <i>mgmt-name</i>	Specifies the MGMT port for the oob option used by the Telnet client.

Defaults


N/A

Command
Mode

Privileged EXEC mode

Usage Guide

This command is used to log in a telnet server.

-  The **/vrf** keyword only applies to the RSR series of routers.
- The **/ipv6** keyword only applies to IPv6-supported devices, such as S3760, S57 and S86.

Configuration
Examples

The following example sets telnet to IPv4 address 192.168.1.11. The port number is the default, and the source interface is Gi 0/1. The queried VRF routing table is vpn1.

```
Ruijie# telnet 192.168.1.11 /source-interface gigabitEthernet 0/1 /vrf vpn1
```

The following example sets telnet to IPv6 address 2AAA:BBBB::CCCC.

```
Ruijie# telnet 2AAA:BBBB::CCCC
```

The following example sets telnet to IPv4 address 192.168.1.1 and specifies the MGMT port for the oob option used by the Telnet client.

```
Ruijie# telnet oob 192.168.1.1 via mgmt 0
```

Related
Commands

Command	Description
---------	-------------

ip telnet source-interface	Specifies the IP address of the interface as the source address for Telnet connection.
show sessions	Displays the currently established Telnet sessions.
exit	Exits current connection.

Platform
Description

N/A

2.51 username

Use this command to set a local username and optional authorization information.. Use the **no** form of this command to restore the default setting.

username *name* [**login mode** { **aux** | **console** | **ssh** | **telnet** }] [**online amount** *number*]
[**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**]
[**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string*]

no username *name*

Parameter
Description

Parameter	Description
<i>name</i>	Username
login mode	Sets the login mode.
aux	Sets the login mode to aux.
console	Sets the login mode to console.
ssh	Sets the login mode to ssh.
telnet	Sets the login mode to telnet.
online amount <i>number</i>	Sets the amount of users online simultaneously.
permission <i>oper-mode path</i>	Sets the permission on the specified file. <i>op-mode</i> refers to the operation mode and <i>path</i> to the file or the directory path.
privilege <i>privilege-level</i>	Sets the privilege level, in the range from 0 to 15.
reject remote-login	Confines the account to remote login.
web-auth	Confines the account to web authentication.
pwd-modify	Allows the web authentication user of this account to change the password. It works only when the web-auth command is configured.
nopassword	The account is not configured with a password.
password [0 7] <i>text-string</i>	If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted. The password is in plain text by default.

Defaults

N/A

Command
Mode

Global configuration mode

Usage Guide This command is used to establish a local user database for authentication.

- i** If encryption type is 7, the cipher text you enter should contain seven characters to be valid. In general, do not set the encryption type 7. Instead, specify the type of encryption as 7 only when the encrypted password is copied and pasted.

Configuration The following example configures a username and password and binds the user to level 15.

Examples Ruijie(config)# username test privilege 15 password 0 pw15

The following example configures the username and password exclusive to web authentication.

Ruijie(config)# username user1 web-auth password 0 pw

The following example configures user test with read and write permissions on all files and directories.

Ruijie(config)# username test permission rw /

The following example configures user test with read, write and execute permissions on all files and directories except the config.text file.

Ruijie(config)# username test permission n /config.text

Ruijie(config)# username test permission rwx /

Related Commands

Command	Description
login local	Enables local authentication

Platform

N/A

Description

2.52 username export

Use this command to export user information to the file.

username export filename

Parameter Description

Parameter	Description
filename	The file name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to export user information to the file.

Configuration

The following example exports user information to the file.

Examples

Ruijie# username export user.csv

Related Commands	Command	Description
	N/A	N/A

**Platform
Description** N/A

2.53 username import

Use this command to import user information from the file.

username import *filename*

Parameter Description	Parameter	Description
	<i>filename</i>	

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide This command is used to import user information from the file.

Configuration The following example imports user information from the file.

Examples Ruijie# username import user.csv

Related Commands	Command	Description
	N/A	N/A

**Platform
Description** N/A

2.54 write

Use this command to save **running-config** at a specified location.

write [**memory** | **terminal**]

Parameter Description	Parameter	Description
	memory	

terminal	Displays the system configuration, which is equivalent to show running-config .
-----------------	--

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Despite the presence of alternative commands, these commands are widely used and accepted. Therefore, they are reserved to facilitate user operations.

The system automatically creates the specified file and writes it into system configuration if the device that stores the file exists;

The system will ask you whether to save the current configuration in default boot configuration file /config.text and perform an action as required if the device that stores the file does not exist possibly because the boot configuration file is stored on a removable storage device such as USB drive or SD card, and the device has not been loaded when you run the **write [memory]** command.

Configuration The following example saves **running-config** at a specified location.

Examples

```
Ruijie# write
Building configuration...
[OK]
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3 LINE Commands

3.1 access-class

Use this command to control login into the terminal through IPv4 ACL. Use the **no** form of this command to restore the default setting.

access-class { *access-list-number* | *access-list-name* } { **in** | **out** }

no access-class { *access-list-number* | *access-list-name* } { **in** | **out** }

Parameter Description	Parameter	Description
	<i>access-list-number</i>	Specifies the ACL number. Standard IP ACL number is from 1 to 99 and from 1300 to 1999. Extended IP ACL number is from 100 to 199 and from 2000 to 2699.
	<i>access-list-name</i>	Specifies the ACL name.
	in	Filters the incoming connections.
	out	Filters the outgoing connections.

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example uses ACL 20 to filter the incoming connections in line VTY 0 5.

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)access-list 20 in
```

The following example uses the ACL named "test" to filter the outgoing connections in line VTY 6 7.

```
Ruijie(config)# line vty 6 7
Ruijie(config-line)access-list test out
```

Related Commands	Command	Description
	show running	Displays status information

Platform Description N/A

3.2 accounting commands

Use this command to enable command accounting in the line. Use the **no** form of this command to restore the default setting.

accounting commands *level* { **default** | *list-name* }

no accounting commands *level*

Parameter Description	Parameter	Description
	<i>level</i>	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
	default	Default authorization list name.
	<i>list-name</i>	Optional list name.

Defaults This function is disabled by default.

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA command accounting first, and then apply it on the line.

Configuration Examples The following example enables command accounting in line VTY 1 and sets the command level to 15.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting commands 15 default start-stop group tacacs+
Ruijie(config)# line vty 1
Ruijie(config-line)# accounting commands 15 default
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.3 accounting exec

Use this command to enable user access accounting in the line. Use the **no** form of this command to restore the default setting.

accounting exec { **default** | *list-name* }

no accounting exec

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
default	Default authorization list name.
<i>list-name</i>	Optional list name.

Defaults This function is disabled by default.

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA EXEC accounting first, and then apply it on the line.

Configuration The following example enables user access accounting in line VTY 1.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting exec default start-stop group radius
Ruijie(config)# line vty 1
Ruijie(config-line)# accounting exec default
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.4 authorization commands

Use this command to enable authorization on commands, Use the **no** form of this command to restore the default setting.

authorization commands *level* { **default** | *list-name* }

no authorization commands *level*

Parameter Description	Parameter	Description
	<i>level</i>	Command level ranging from 0 to 15. The command of this level is executed after authorization is performed.
	default	Default authorization list name,
	<i>list-name</i>	Optional list name.

Defaults This function is disabled by default.

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA authorization first, and then apply it on the line.

Configuration The following example enables authorization on commands of level 15 in line VTY 1.

Examples

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authorization commands 15 default group tacacs+
Ruijie(config)# line vty 1
Ruijie(config-line)# authorization commands 15 default
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.5 authorization exec

Use this command to enable EXEC authorization for the line. Use the **no** form of this command to restore the default setting.

authorization { **default** | *list-name* }
no authorization exec

**Parameter
Description**

Parameter	Description
default	Default authorization list name,
<i>list-name</i>	Optional list name.

Defaults This function is disabled by default,

Command Line configuration mode
Mode

Usage Guide This function is used together with AAA authorization. Configure AAA EXEC authorization first, and then apply it on the line.

Configuration The following example performs EXEC authorization to line VTY 1.

Examples

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authorization exec default group radius
Ruijie(config)# line vty 1
Ruijie(config-line)# authorization exec default
```

Related

Command	Description
---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

3.6 clear line

Use this command to clear connection status of the line.

clear line { **console** *line-num* | **vtty** *line-num* | *line-num* }

Parameter Description	Parameter	Description
	console	Clears connection status of the console line.
	vtty	Clears connection status of the virtual terminal line.
	<i>line-num</i>	Specifies the line to be cleared.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear connection status of the line and restore the line to the unoccupied status to create new connections.

Configuration Examples The following example clears connection status of line VTY 13. The connected session on the client (such as Telnet and SSH) in the line is disconnected immediately.

```
Ruijie# clear line vty 13
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.7 disconnect-character

Use this command to set the hot key that disconnects the terminal service connection. Use the **no** form of this command to restore the default setting.

disconnect-character *ascii-value*

no disconnect-character

Parameter Description	Parameter	Description
	<i>ascii-value</i>	ASCII decimal value of the hot key that disconnects the terminal service connection, in the range from 0 to 255.

Defaults The default hot key is **Ctrl+D** and the ASCII decimal value is 0x04.

Command Mode Line configuration mode

Usage Guide This command is used to set the hot key that disconnects the terminal service connection. The hot key cannot be the commonly used ASCII node such as characters ranging from a to z, from A to Z or numbers ranging from 0 to 9. Otherwise, the terminal service cannot operate properly.

Configuration Examples The following example sets the hot key that disconnects the terminal service connection on line VTY 0 5 to **Ctrl+E** (0x05).

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# disconnect-character 5
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.8 escape-character

Use this command to set the escape character for the line. Use the **no** form of this command to restore the default setting.

escape-character *escape-value*

no escape-character

Parameter Description	Parameter	Description
	<i>escape-value</i>	Sets the ASCII value corresponding to the escape character for the line, in the range from 0 to 255.

Defaults The default escape character is **Ctrl+^** (**Ctrl+Shift+6**) and the ASCII decimal value is 30.

Command Mode Line configuration mode

Usage Guide After configuring this command, press the key combination of the escape character and then press x,

the current session is disconnected to return to the original session.

Configuration The following example sets the escape character for the line to 23 (**Ctrl+w**).

Examples

```
Ruijie(config)# line vty 0
Ruijie(config-line)# escape-character 23
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

3.9 exec

Use this command to enable the line to enter the command line interface. Use the **no** form of this command to disable the function.

exec

no exec

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

**Command
Mode**

Line configuration mode

Usage Guide

The **no exec** command is used to ban the line from entering the command line interface. You have to enter the command line interface through other lines,

Configuration The following example bans line VTY 1 from entering the command line interface.

Examples

```
Ruijie(config)# line vty 1
Ruijie(config-line)# no exec
Ruijie# show users
```

Line	User	Host(s)	Idle	Location
* 0 con 0	---	idle	00:00:00	---
1 vty 0	---	idle	00:01:03	20.1.1.2
3 vty 2	---	idle	00:00:13	20.1.1.2

Related

Command	Description
---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

3.10 history

Use this command to enable command history for the line or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

history [size size]

no history

no history size

Parameter Description	Parameter	Description
	size size	The number of commands, in the range from 0 to 256.

Defaults This function is enabled by default, The default *size* is 10.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the number of commands in the command history to 20 for line VTY 0 5.

```
Ruijie(config)# line vty 0 5
```

```
Ruijie(config-line)# history size 20
```

The following example disables the command history for line VTY 0 5.

```
Ruijie(config)# line vty 0 5
```

```
Ruijie(config-line)# no history
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.11 ipv6 access-class

Use this command to configure access to the terminal through IPv6 ACL. Use the **no** form of this

command to restore the default setting.

ipv6 access-class *access-list-name* { **in** | **out** }

no ipv6 access-class *access-list-name* { **in** | **out** }

Parameter Description	Parameter	Description
	<i>access-list-name</i>	Specifies the ACL name.
	in	Filters the incoming connections.
	out	Filters the outgoing connections.

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example uses the ACL named “test” to filter the outgoing IPv6 connections in line VTY 0 4.

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)ipv6 access-list test out
```

Related Commands	Command	Description
	show running	Displays status information

Platform Description N/A

3.12 length

Use this command to set the screen length for the line. Use the **no** form of this command to restore the default setting.

length *screen-length*

no length

Parameter Description	Parameter	Description
	<i>screen-length</i>	Sets the screen length, in the range from 0 to 512.

Defaults The default is 24.

Command Mode Line configuration mode

Usage Guide N/A

Configuration The following example sets the screen length to 10.

Examples

```
Ruijie(config-line)# length 10
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

3.13 line

Use this command to enter the specified LINE mode.

line [**console** | **vty**] *first-line* [*last-line*]

**Parameter
Description**

Parameter	Description
console	Console port
vty	Virtual terminal line, applicable for telnet/ssh connection.
<i>first-line</i>	Number of first-line to enter
<i>last-line</i>	Number of last-line to enter

Defaults N/A

**Command
Mode** Global configuration mode

Usage Guide This command is used to enter the specified LINE mode.

Configuration The following example enters the LINE mode from LINE VTY 1 to 3:

Examples

```
Ruijie(config)# line vty 1 3
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

3.14 line vty

Use this command to increase the number of VTY connections currently available. Use the **no** form of this command to restore the default setting.

line vty *line-number*

no line vty *line-number*

Parameter Description	Parameter	Description
	<i>line-number</i>	The number of VTY connections, in the range from 0 to 35.

Defaults By default, there are five available VTY connections, numbered 0 to 4.

Command Mode Global configuration mode.

Usage Guide When you need to increase or decrease the number of available VTY connections, use the above commands.

Configuration Examples The following example increases the number of available VTY connections to 20. The available VTY connections are numbered 0 to 19.

```
Ruijie(config)# line vty 19
```

Decrease the number of available VTY connections to 10. The available VTY connections are numbered 0-9.

```
Ruijie(config)# line vty 10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.15 location

Use this command to configure the line location description. Use the **no** form of this command to restore the default setting.

location *location*

no location

Parameter Description	Parameter	Description
	<i>location</i>	Line location description

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration The following example describes the line location as Switch's Line VTY 0.

Examples

```
Ruijie(config)# line vty 0
Ruijie(config-line)# location Switch's Line Vty 0
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.16 monitor

Use this command to enable log display on the terminal. Use the **no** form of this command to restore the default setting,

monitor

no monitor

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration The following example enables log display on the terminal in VTY line 0 5.

Examples

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# monitor
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.17 privilege level

Use this command to set the privilege level for the line. Use the **no** form of this command to restore the default setting.

privilege level *level*

no privilege level

**Parameter
Description**

Parameter	Description
<i>level</i>	Privilege level, in the range from 0 to 15.

Defaults The default is 1.

**Command
Mode** Line configuration mode

Usage Guide N/A

Configuration The following example sets the privilege level for the line VTY 0 4 to 14.

Examples

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)privilege level 14
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

3.18 refuse-message

Use this command to set the login refusal message for the line. Use the **no** form of this command to restore the default setting.

refuse-message [*c message c*]

no refuse-message

**Parameter
Description**

Parameter	Description
<i>c</i>	Delimiter of the login refusal message, which is not allowed within the

	message.
<i>message</i>	Login refusal message.

Defaults N/A

Command Mode Line configuration mode

Usage Guide This command is used to set the login refusal message for the line. The characters entered after the ending delimiter are discarded directly, The login refusal message is displayed when the user has been refused to login.

Configuration Examples The following example sets the login refusal message for the line to “Unauthorized user cannot login to the ruijie device”.

```
Ruijie(config-line)#vacant-message @ Unauthorized user cannot login to the
ruijie device @
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.19 show history

Use this command to display the command history of the line.

show history

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the command history of the line.

```
Ruijie# show history
exec:
sh privilege
```

```
sh run
show user
sh user all
show history
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.20 show line

Use this command to display line configuration.

show line { **console** *line-num* | **vt** *line-num* | *line-num* }

**Parameter
Description**

Parameter	Description
console	Displays configuration for the console line.
vt	Displays configuration for the virtual terminal line.
<i>line-num</i>	Displays the line.

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays configuration for the console port.

Examples

```
Ruijie# show line console 0
CON      Type      speed  Overruns
* 0      CON      9600   45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape Disconnect Activation
                ^^x      none      ^M
Timeouts:      Idle EXEC   Idle Session
                never      never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output: 395756 bytes
Data overflow: 27697 bytes
```

```
stop rx interrupt: 0 times
```

Field	Description
CON	Terminal type. CON indicates console; 0 indicates terminal line number and * ahead of the number means that the terminal is in use.
Type	Terminal type, including CON, AUX, TTY, and VTY.
speed	Asynchronous speed.
Overruns	The number of overrun errors received by the flash.
Line 0	Terminal line number.
Location: ""	Line location configuration.
Type: "vt100"	Compatibility standard.
Special Chars	Special characters, including Escape, Disconnect, and Activation characters.
Timeouts	Timeout value; "never" indicates no timeout.
History	Whether to enable command history; the number of commands in the command history.
Total input	Data volume received from the drive.
Total output	Date volume sent to the drive.
Data overflow	Overflowing data volume.
stop rx interrupt	Data reception interruption times.

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

3.21 show privilege

Use this command to display the privilege level of the line.

show privilege

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the privilege level of the line.

Examples

```
Ruijie# show privilege
Current privilege level is 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.22 show users

Use this command to display the login user information.

show users [all]

Parameter Description	Parameter	Description
		all

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the information about users logging into the line,

Examples

```
Ruijie# show users
Line          User          Host(s)        Idle           Location
-----
0 con 0      ---          idle           00:00:46      ---
1 vty 0      ---          idle           00:00:29      20.1.1.2
* 2 vty 1    ---          idle           00:00:00      20.1.1.2
```

The following example displays all line user information,

```
Ruijie(config)# show users all
Line          User          Host(s)        Idle           Location
-----
0 con 0      ---          idle           00:00:49      ---
1 vty 0      ---          idle           00:00:32      20.1.1.2
* 2 vty 1    ---          idle           00:00:00      20.1.1.2
```

3 vty 2	---	00:00:00	---
4 vty 3	---	00:00:00	---
5 vty 4	---	00:00:00	---
6 vty 5	---	00:00:00	---

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.23 speed

Use this command to configure the baud rate for the specified line. Use the **no** form of this command to restore the default setting,

speed *baudrate*

no speed

Parameter Description	Parameter	Description
		<i>baudrate</i>

Defaults The default is 9600.

Command Mode LINE configuration mode

Usage Guide N/A

Configuration Examples The following example sets the baud rate to 115200,

```
Ruijie(config-line)# speed 115200
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.24 terminal escape-character

Use this command to set the escape character for the current terminal. Use the **no** form of this

command to restore the default setting.

terminal escape-character *escape-value*

terminal no escape-character

Parameter Description	Parameter	Description
	<i>escape-value</i>	Sets the ASCII value corresponding to the escape character for the current terminal, in the range from 0 to 255.

Defaults The default escape character is **Ctrl+^ (Ctrl+Shift+6)** and the ASCII decimal value is 30.

Command Mode Privileged EXEC mode

Usage Guide After configuring this command, press the key combination of the escape character and then press x, the current session is disconnected to return to the original session.

Configuration Examples The following example sets the escape character for the current terminal to 23 (**Ctrl+w**).

```
Ruijie# terminal escape-character 23
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.25 terminal history

Use this command to enable command history for the current terminal or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

terminal history [*size size*]

terminal no history

terminal no history size

Parameter Description	Parameter	Description
	<i>size size</i>	Sets the number of commands, in the range from 0 to 256.

Defaults This function is enabled by default, The default *size* is 10.

Command Privileged EXEC mode

Mode**Usage Guide** N/A**Configuration Examples** The following example sets the number of commands in the command history to 20 for the current terminal.

```
Ruijie# terminal history size 20
```

The following example disables the command history for the current terminal.

```
Ruijie# terminal no history
```

Related Commands

Command	Description
N/A	N/A

Platform N/A**Description**

3.26 terminal length

Use this command to set the screen length for the current terminal. Use the **no** form of this command to restore the default setting.**terminal length** *screen-length***terminal no length****Parameter Description**

Parameter	Description
<i>screen-length</i>	Sets the screen length, in the range from 0 to 512.

Defaults The default is 24.**Command Mode** Privileged EXEC mode**Usage Guide** N/A**Configuration Examples** The following example sets the screen length for the current terminal to 10.

```
Ruijie# terminal length 10
```

Related Commands

Command	Description
N/A	N/A

Platform N/A**Description**

3.27 terminal location

Use this command to configure location description for the current device. Use the **no** form of this command to restore the default setting.

terminal location *location*

terminal no location

Parameter Description	Parameter	Description
	<i>location</i>	Configures location description of the current device.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures location description of the current device as "Switich's Line Vty 0".

```
Ruijie# terminal location Switich's Line Vty 0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.28 terminal speed

Use this command to configure the baud rate for the current terminal. Use the **no** form of this command to restore the default setting,

terminal speed *baudrate*

terminal no speed

Parameter Description	Parameter	Description
	<i>baudrate</i>	Sets the baud rate, in the range from 9600 to 115200.

Defaults The default is 9600.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example sets the baud rate for the current terminal to 115200,

Examples

```
Ruijie# terminal speed 115200
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.29 terminal width

Use this command to set the screen width for the terminal.

terminal width *screen-width*

terminal no width

Parameter Description	Parameter	Description
	<i>screen-width</i>	

Defaults The default is 79.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example sets the screen width for the terminal to 10.

Examples

```
Ruijie# terminal width 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.30 timeout login

Use this command to set the login authentication timeout for the line. Use the **no** form of this

command to restore the default setting.

timeout login response *seconds*

no timeout login response

Parameter Description	Parameter	Description
	response	The time period during which the line waits for the user to enter any message.
	<i>seconds</i>	Timeout value, in the range from 1 to 300 in the unit of seconds.

Defaults The default is 30.

Command Mode Line configuration mode

Usage Guide N/A

Configuration The following example sets the login authentication timeout to 300 seconds for line VTY 0 5.

Examples

```
Ruijie(config)# line vty 0 5
Ruijie(config-line) login timeout response 300
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.31 transport input

Use this command to set the specified protocol under Line that can be used for communication. Use the **no** form of this command to restore the default setting.

transport input { **all** | **ssh** | **telnet** | **none** }

no transport input { **all** | **ssh** | **telnet** | **none** }

Parameter Description	Parameter	Description
	all	Allows all the protocols under Line to be used for communication
	ssh	Allows only the SSH protocol under Line to be used for communication
	telnet	Allows only the Telnet protocol under Line to be used for communication
	none	Allows none of protocols under Line to be used for communication

Defaults all, **ssh** and **telnet** protocols are allowed.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example specifies that only the Telnet protocol is allowed to login in line vty 0 4.

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)transport input ssh
```

Related Commands

Command	Description
show running	Displays status information

Platform N/A

Description

3.32 vacant-message

Use this command to set the logout message. Use the **no** form of this command to restore the default setting.

vacant-message [*c message c*]

no vacant-message

Parameter Description

Parameter	Description
<i>c</i>	Delimiter of the logout message, which is not allowed within the message.
<i>message</i>	Logout message.

Defaults N/A

Command Mode Line configuration mode

Usage Guide This command is used to set the logout message for the line. The characters entered after the ending delimiter are discarded directly, The logout message is displayed when the user logs out.

Configuration Examples The following example sets the logout message to "Logout from the ruijie device".

```
Ruijie(config-line)#vacant-message @ Logout from the ruijie device @
```

Related

Command	Description
---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

3.33 width

Use this command to set the screen width for the line. Use the **no** form of this command to restore the default setting,

width *screen-width*

no width

Parameter Description	Parameter	Description
	<i>screen-width</i>	Sets the screen width for the line, in the range from 0 to 256,

Defaults The default is 79.

Command Line configuration mode

Mode

Usage Guide N/A

Configuration The following example sets the screen width for the line to 10.

Examples Ruijie(config-line)# width 10

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4 File System Commands

4.1 cd

Use this command to set the present directory for the file system.

```
cd [ filesystem: ] [ directory ]
```

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of filesystem, followed by a colon (:). The filesystem includes flash: , usb: , sd: and tmp: .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default directory is the flash root directory.

Command Privileged EXEC mode.

Mode The specified path of the file system support URLs. For details of URL prefixes, see description of the **copy** command.

Usage Guide Change the above parameter to the directory you want to enter. Use the **pwd** command to view the present directory.

Configuration

Examples

Related	Command	Description
Commands	pwd	Displays the present word directory.

Platform N/A.

Description

4.2 copy

Use this command to copy a file from the specified source directory to the specified destination directory.

```
copy source-url destination-url
```

Parameter	Parameter	Description
Description	<i>source-url</i>	Source file URL, which can be local or remote.
	<i>destination-url</i>	Destination file URL, which can be local or remote.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide when the file to be copied exists on the target URL, the target file system determines the action, such as error report, overwrite, or offering you the choice.

The following table lists the URL:

Prefix	Description
running-config	Running configuration file.
startup-config	startup configuration file.
flash:	local FLASH file system.
tftp:	The URL of TFTP network server, in the format as follows: tftp:[[/location]/directory]/filename
oob_tftp: [via mgmt. {number}]	The URL of TFTP network server connected with the Out-of-Band port, If there are multiple MGMT ports, you can specify one.
xmodem:	Files on the network device using the xmodem protocol.

Configuration Examples The following example copies the netconfig file from device 192.168.64.2 to the FLASH disk and the netconfig file exists locally.

```
Ruijie#copy tftp://192.168.64.2/netconfig flash:/netconfig
The file [flash:/netconfig] exists, override it? [Y/N]: y
Copying: !!!!!!!!

Accessing tftp://192.168.64.2/netconfig finished, 2399bytes prepared
Flushing data to flash:/netconfig..
Flush data done
```

Related Commands	Command	Description
	delete	Deletes the file.
	rename	Renames the file.
	dir	Displays the file list of the specified directory.

Platform Description N/A

4.3 delete

Use this command to delete the files in the present directory.

delete [*filesystem:*] *file-url* [*/force* | */recursive*]

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system

	includes flash: , usb: , sd: and tmp: .
<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
/force	Deletes the file without the user's confirmation.
/recursive	Deletes all files in a directory recursively, including the directory itself.

Defaults The default *filesystem:* is **flash:**.

Command Privileged EXEC mode.

Mode

Usage Guide This command is used to delete the specified file in the URL. This command supports deleting the files stores in the local storage media, i.e., the URL must be one of the flash:/ usb0:/ or usb1:/ slave/. If the prefix is not specified in the URL, it indicates to delete the file in the system.

In VSU mode, URLs do not support sw1-m1-disk0:/ series. For details of the supported prefixes, see the description of the **copy** command.

This command does not support wildcard.

Configuration The following example deletes the fstab file on the FLASH disk.

Examples

```
Ruijie#pwd
flash:/
Ruijie#dir
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  fstab
 2  -rw-     4096   Jan 03 2012 12:32:09   rc.d
 3  -rw-  10485760   Jan 03 2012 18:13:37   rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Ruijie#delete flash:/fstab
Ruijie#dir
Directory of flash:/
 1  -rw-      4096   Jan 03 2012 12:32:09   rc.d
 2  -rw-  10485760   Jan 03 2012 18:13:37   rpmdb
2 files, 0 directories
10,489,856 bytes total (13,192,992 bytes free)
```

The following example deletes the non-null file on the FLASH disk recursively.

```
Ruijie#pwd
flash:/
Ruijie#dir
Directory of flash:/
 1  drwx           0  Thu Jan  1 02:02:25 1970  file
 2  -rw-     610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 1 directory
58,720,256 bytes total (28,577,792 bytes free)
```

```
Ruijie#delete /recursive flash:/file
Ruijie#dir
Directory of flash:/
 1 -rw-      610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 0 directories
58,720,256 bytes total (31,358,976 bytes free)
```

Related Commands	Command	Description
	copy	Copies the file.
	dir	Displays the file list of the specified directory.

Platform N/A
Description

4.4 dir

Use this command to display the files in the present directory.

dir [*filesystem:*] [*directory*]

Parameter Description	Parameter	Description
	<i>filesystem</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: , sd: and tmp: .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults By default, only the information under the present working path is displayed.

Command Mode Privileged EXEC mode.

Usage Guide Enter the specified directory to show the information of all the files in that directory. If no parameter is specified, the information of the files in the present directory is shown by default.
This command does not support wildcard.

Configuration Examples The following example displays the file information of the root directory in the FLASH disk.

```
Ruijie#dir flash:/
Directory of flash:/
1  -rw-      336  Jan 03 2012 18:53:42  fstab
2  -rw-      4096  Jan 03 2012 12:32:09  rc.d
3  -rw-    10485760  Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

Field	Description
1, 2, 3...	Index number
-rw-	Permissions on a file include: <ul style="list-style-type: none"> ● d: directory ● r: read ● w: write ● x: executable
10485760	File size
rpmdb	File name
files	File number
directories	Directory number
total	Total size
free	Available space

Related Commands	Command	Description
	pwd	Displays the present directory.
	cd	Sets the present directory of the file system.

Platform N/A.
Description

4.5 eject

Use this command to remove the USB or SD disk.

eject [usb0 | sd0]

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example removes the USB disk.

Examples

```
Ruijie#eject ?
sd0  Eject sd disk 0
usb0 Eject usb disk 0

Ruijie#eject usb0
Ruijie#
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

4.6 erase

Use this command to erase the device or file that doesn't have a file system.

erase *filesystem*

Parameter	Parameter	Description
Description	<i>filesystem:</i>	Name of the file system, followed by a colon (:). For example, usb0:.

Defaults N/A

Command Privileged EXEC mode
Mode

Usage Guide N/A

Configuration The following example erases the USB filesystem.

Examples

```
Ruijie#erase usb0:
Sure to erase usb0:? [Y/N] y
Erasing disk usb0 ...
Erase disk usb0 done!
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

4.7 file

Use this command to display the information about a file.

file [*filesystem:*] *file-url*

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: , sd: and tmp: .

<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
-----------------	---

Defaults The default *filesystem*: is **flash:**.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the information about gcc executable file.

Examples

```
Ruijie#file flash:/gcc
/usr/bin/gcc-4.6: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV),
dynamically linked (uses shared libs), for GNU/Linux 2.6.15, stripped
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.8 file prompt

Use this command to set the prompt mode.

file prompt [noisy | quiet]

Parameter Description	Parameter	Description
	noisy	Displays prompt for all operation.
	quiet	Displays prompt rarely.

Defaults The default mode is noisy.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example sets the prompt mode to noisy.

Examples

```
Ruijie#file prompt noisy
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.9 mkdir

Use this command to create a directory.

mkdir [*filesystem:*] *directory*


Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: , sd: and tmp: .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem:* is **flash:**.
The default *directory* is the root directory.

Command Privileged EXEC mode.

Mode

Usage Guide Simply enter the name of the directory you want to create (including the path).

 If the created file has been existed, the creation will fail. If the upper-level for the directory to be created is inexistent, it fails to create the specified directory. For example, if the directory of flash:/backup is inexistent, the creation of the directory of flash:/backup/temp will fail. The solution is that the directory of flash:/backup shall be created before the creation of the directory of flash:/backup/temp.

Configuration The following example creates a directory named newdir:

Examples

```
Ruijie#dir
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  fstab
 2  -rw-     4096   Jan 03 2012 12:32:09  rc.d
 3  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
Ruijie#mkdir newdir
Created dir flash:/newdir
Ruijie#dir
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  fstab
 2  -rw-     4096   Jan 03 2012 12:32:09  rc.d
 3  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
```

```
4 drw-      4096   Jan 03 2012 18:13:37 newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
```

Related Commands	Command	Description
	rmdir	Deletes the directory.
	pwd	Displays the present directory.
Platform	N/A	
Description		

4.10 more

Use this command to display the content of a file.

more [*/ascii* | */binary*] [*filesystem:*] *file-url*

Parameter	Parameter	Description
Description	<i>/ascii</i>	Displays the file content in the ASCII format.
	<i>/binary</i>	Displays the file content in the
	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: , sd: and tmp: .
	<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The file is displayed in its own format by default.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the content of the netconfig file under root directory of FLASH disk.

```
Ruijie#more flash:/netconfig
#
# The network configuration file. This file is currently only used in
# conjunction with the TI-RPC code in the libtirpc library.
#
# Entries consist of:
#
#     <network_id> <semantics> <flags> <protopfamily> <protoname> \
#         <device> <nametoaddr_libs>
#
# The <device> and <nametoaddr_libs> fields are always empty in this
# implementation.
```

#						
udp	tpi_clts	v	inet	udp	-	-
tcp	tpi_cots_ord	v	inet	tcp	-	-
udp6	tpi_clts	v	inet6	udp	-	-
tcp6	tpi_cots_ord	v	inet6	tcp	-	-
rawip	tpi_raw	-	inet	-	-	-
local	tpi_cots_ord	-	loopback	-	-	-

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.11 pwd

Use this command to display the working path.

pwd

Parameter	Parameter	Description
Description	N/A.	N/A.

Defaults N/A.

Usage Guide This command displays the present working path

Configuration

Examples

Related	Command	Description
Commands	cd	Changes the file system in the present directory.

Platform N/A.

Description

4.12 rename

Use this command to move or rename the specified file.

rename *src-url dst-url*

Parameter	Parameter	Description
Description	<i>src-url</i>	The source file URL to move.
	<i>dst-url</i>	The URL of the destination file or directory.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example renames the fstab file in the root directory on the FLASH disk as new-fstab.

Examples

```
Ruijie#dir
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  fstab
 2  -rw-     4096   Jan 03 2012 12:32:09   rc.d
 3  -rw-   10485760   Jan 03 2012 18:13:37   rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Ruijie#rename flash:/fstab flash:/new-fstab
Renamed file flash:/new-fstab
Ruijie#dir
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  new-fstab
 2  -rw-     4096   Jan 03 2012 12:32:09   rc.d
 3  -rw-   10485760   Jan 03 2012 18:13:37   rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

Related Commands

Command	Description
delete	Deletes the file.
copy	Copies the file.

Platform N/A

Description

4.13 rmdir

Use this command to delete an empty directory.

rmdir [*filesystem:*] *directory*

Parameter Description

Parameter	Description
<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: , sd: and tmp: .
<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem:* is **flash:**.

Command Mode Privileged EXEC mode.

Usage Guide This command does not support the wildcards, and the directory to be deleted must be empty. Since this command supports abbreviations, you can also use the **rm** command to delete empty directories.

Configuration The following example deletes the null test directories.

Examples

```
Ruijie#mkdir newdir
Ruijie#dir
Directory of flash:/
1  -rw-      336  Jan 03 2012 18:53:42  fstab
2  -rw-     4096  Jan 03 2012 12:32:09  rc.d
3  -rw-  10485760  Jan 03 2012 18:13:37  rpmdb
4  drw-      4096  Jan 03 2012 18:13:37  newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
Ruijie#rmdir newdir
removed dir flash:/newdir
Ruijie#dir
Directory of flash:/
1  -rw-      336  Jan 03 2012 18:53:42  fstab
2  -rw-     4096  Jan 03 2012 12:32:09  rc.d
3  -rw-  10485760  Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
```

Related	Command	Description
Commands	N/A.	N/A.

Platform N/A.

Description

4.14 show disk

Use this command to display USB/Flash information.

show disk sata/usb/flash

Parameter Description	Parameter	Description
	usb	Displays USB information.
	flash	Displays FLASH information.
	sata	Displays hardware information.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays SATA information.

Examples

```
Ruijie#show disk sata
Disk /dev/sda: 160.0 GB, 160039272960 bytes
255 heads, 63 sectors/track, 19457 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

The following example displays USB information.

```
Ruijie#show disk usb
Disk /dev/sdb: 8159 MB, 8159477760 bytes
252 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 15624 * 512 = 7999488 bytes
```

The following example displays FLASH information.

```
Ruijie#show disk flash
Nand flash size: 512MB
Nor flash size: 1MB
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.15 show file systems

Use this command to display the file system information.

show file systems

Parameter Description	Parameter	Description
	N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the file systems supported in the present devices and the available space condition in the file system.

Configuration The following example displays the file system information:

Examples

```
Ruijie#show file systems
```

```

  Size(KB)      Free(KB)      Type  Flags Prefixes
      NA         NA        ram   rw tmp:
      NA         NA    network  rw tftp:
      NA         NA    network  rw oob_tftp:
      NA         NA    xmodem   rw xmodem
    8192        2416        disk   rw flash:
167772160    147772160        disk   rw sata0:
  1048576        548576        disk   rw usb0:
   262144        152144        disk   rw sd0:

```

Field	Description
Size(KB)	File system space, in the unit of KB.
Free(KB)	Available file system space, in the unit of KB.
Type	File system type
Flags	Permissions on the file system include: <ul style="list-style-type: none"> ● ro: read-only ● wo: write-only ● rw: read and write
Prefixes	File system prefix

Related**Commands**

Command	Description
N/A.	N/A.

Platform

N/A.

Description

4.16 show mount

Use this command to display the mounted information.

show mount

Parameter**Description**

Parameter	Description
N/A	N/A

Defaults

N/A

Command

N/A

Mode

Usage Guide N/A

Configuration The following example displays the mounted information.

Examples

```
Ruijie#show mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro,commit=0)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
/dev/sda3 on /hao-share type ext3 (rw,commit=0)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc
(rw,noexec,nosuid,nodev)
```

Field	Description
proc	Source address of mount.
on	-
/proc	Destination address of mount.
type	-
proc	Mount type.
(rw,noexec,nosuid,nodev)	Mount property.

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.17 tftp-client source

Use this command to bind a source IP address or source interface with a TFTP client. Use the **no** or **default** form of this command to restore the default setting.

tftp-client source { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface* }

no tftp-client source { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface* }

default tftp-client source { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface* }

Parameter	Parameter	Description
Description	<i>ip-address</i>	Specifies the IPv4 source address.

<i>ipv6-address</i>	Specifies the IPv6 source address.
<i>interface</i>	Specifies the source interface

Defaults No source interface or IP address is bound with the TFTP client by default.

Command Global configuration mode

Mode

Usage Guide N/A

Configuration The following example binds source IP address 192.168.23.236 with the TFTP client.

Examples Ruijie(config)# tftp-client source ip 192.168.23.236

The following example binds source IPv6 address 2003:0:0::2 with the TFTP client.

Ruijie(config)# tftp-client source ipv6 2003:0:0:0::2

The following example binds source interface gigabitEthernet 0/0 with the TFTP client.

Ruijie(config)# tftp-client source gigabitEthernet 0/0

The following example removes the configuration.

Ruijie(config)# no tftp-client source ip 192.168.23.236

The following example restores the default setting.

Ruijie(config)# default tftp-client source ip 192.168.23.236

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.18 tree

Use this command to display the file tree of the current directory.

tree [*filesystem:*] [*directory*]

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: , sd: and tmp: .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem:* is **flash:**.

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the file tree of flash:/echo

Examples

```
Ruijie#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
|   +-- echo.ko
|   +-- echo.mod.c
|   +-- echo.mod.o
|   +-- echo_module.c
|   +-- echo_module.o
|   +-- echo.o
|   +-- echo_server.c
|   +-- echo_server.o
|   +-- echo_sysfs.c
|   +-- echo_sysfs.h
|   +-- echo_sysfs.o
|   +-- Makefile
|   +-- modules.order
|   +-- Module.symvers
|   +-- msg_fd.c
|   +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_rgos.ko
+-- user_space
    +-- echo_server.c
    +-- echo_server.o
    +-- Makefile
    +-- msg_fd.c
    +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

4.19 verify

Use this command to compute, display and verify Message Digest 5 (MD5).

verify [/md5 md5-value] filesystem: [file-url]

Parameter	Parameter	Description
Description	/md5	Computes and displays MD5.
	md5-value	The file MD5, which is compared with the computed MD5.
	filesystem:	The URL of file system, followed by a colon (:). The file system includes flash: , usb: , sd: and tmp: .
	file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults The default *filesystem:* is **flash:**.

Command Privileged EXEC mode.
Mode

Usage Guide N/A

Configuration The following example computes MD5 of flash:/gcc.

Examples

```
Ruijie#verify flash:/gcc
8b072de7db7affd8b2ef824e7e4d716c
```

The following example computes MD5 of flash:/gcc and makes comparison.

```
Ruijie#verify /md5 8b072de7db7affd8b2ef824e7e4d716c flash:/gcc
%SUCCESS verifying /mnt/flash/gcc = 8b072de7db7affd8b2ef824e7e4d716c
Ruijie#verify /md5 8b072de7db7affd8b2ef824e7e4d71 flash:/gcc
%Error verifying flash:/gcc
Computed signature = 8b072de7db7affd8b2ef824e7e4d716c
Submitted signature = 8b072de7db7affd8b2ef824e7e4d71
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

5 SYS Commands

5.1 calendar set

Use this command to set the hardware calendar.

calendar set { *hour* [*:minute* [*:second*]] } [*month* [*day* [*year*]]]

Parameter Description	Parameter	Description
	<i>hour</i> [<i>:minute</i> [<i>:second</i>]]	Sets hardware time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can be reset. The unspecified parameters keep the current system values.
	<i>month</i>	Sets month. The range is from 1 to 12.
	<i>day</i>	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
	<i>year</i>	Sets year. The range is from 1970 to 2069.


Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide

- The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value. For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **calendar set 12 5** command to change the current time into "2012-05-29 12:33:44".
- If the value of parameter *day* is between 1 and 31, but the current month does not contain that day, the value will be calculated backward. For example, February 2012 has 29 days. If you use the **calendar set 11:30 2 31 2012** command to set the date to February 31, by default, the system adds two days backwards. Therefore, the current hardware time is "2012-03-02 11:30:23".

 The hardware time of the system is used as the UTC time, while the software time of the system refers to the local time of the device.

 This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters.


```
Ruijie# calendar set 6
06:41:39 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.

```
Ruijie# calendar set 6:42
06:42:27 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
Ruijie# calendar set 18 3 2
18:43:05 UTC Fri, Mar 2, 2012
```

 Because the *hour* parameter is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month) and **2** (day).

Check Method -

Platform -

Description -

5.2 clock read-calendar

Use this command to enable the system to synchronize the software time with the hardware time.

clock read-calendar

Parameter Description	Parameter	Description
	-	-

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported. After you configure this command, the system will synchronize the software time with the current hardware time according to the time zone and summer time settings of the device.

Configuration Examples The following example enables the system to synchronize the software time with the hardware time.

```
Ruijie# clock read-calendar
Set the system clock from the hardware time.
```

Check Method -

Platform -
Description -

5.3 clock set

Use this command to set the system software clock.

```
clock set { hour [ :minute [ :second ] ] } [ month [ day [ year ] ] ]
```


Parameter Description	Parameter	Description
	<i>hour</i> [<i>:minute</i> [<i>:second</i>]]	Sets software time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can reset. The unspecified parameters keep the current system values.
	<i>month</i>	Sets month. The range is from 1 to 12.
	<i>day</i>	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
	<i>year</i>	Sets year. The range is from 1970 to 2069.

Defaults -


Command Mode Privileged EXEC mode

Default Level -

Usage Guide 1. The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value.

 For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **clock set 12 5** command to change the current time into "2012-05-29 12:33:44".

2. If the value of parameter *day* is between 1 and 31, but the current month does not contain that day, the value will be calculated backward.

 For example, February 2012 has 29 days. If you use the **clock set 11:30 2 31 2012** command to set the date to February 31, by default, the system adds two days backward. Therefore, the current hardware time is "2012-03-02 11:30:23".

This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters.

```
Ruijie# clock set 6
```

```
06:48:13 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.


```
Ruijie# clock set 6:42
```

```
06:42:31 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
Ruijie# clock set 18 3 2
```

```
18:42:48 CST Fri, Mar 2, 2012
```

 Because the *hour* parameter in this command is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month) and **2** (day).

Check Method -

Platform -

Description -

5.4 clock summer-time

Use this command to set the summer time.

```
clock summer-time zone start start-month [week|last] start-date hh:mm end end-month [week|last] end-date hh:mm [ ahead hours-offset [minutes-offset ]
```

Use this command to disable the summer time.

```
no clock summer-time
```

Parameter Description	Parameter	Description
	zone	Summer time name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The summer time name contains 3 to 31 characters.
	start	Indicates the start time of the summer time.
	<i>start-month</i>	Start month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Febr and FebRu.
	<i>week</i>	Start week in the start month. The range is from 1 to 5.
	last	The last week of the specified month.
	<i>start-date</i>	Day in the start week of the start month. Value range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Web and WeDne.
	hh:mm	Time, in the format of hour : minute.
	end	Indicates the end time of the summer time.
	<i>end-month</i>	End month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you may enter an incomplete word, for example, Febr and FebRu.
	ahead	Indicates how much time for the summer time ahead of the standard time during the effective period of the summer time. By default, the summer time is one hour ahead of the standard time.
	<i>hours-offset</i>	Hours ahead of the standard time. The range is from 0 to 12. You are not allowed to set it to 00:00.
	<i>minutes-offset</i>	Minutes ahead of the standard time. The range is from 0 to 59. If <i>hours-offset</i> has been set to 0, you are not allowed to set <i>minutes-offset</i> to 0.

Defaults -

Command Mode Global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples Assume that the time zone name of your living place is ABC and the standard time is 8:15 ahead of UTC, namely, GMT+08:15. The summer time period starts from the first Saturday in February to the third Monday in May and the summer time is 01:20 ahead of the standard time. In this case, the summer time is

09:35 ahead of the UTC time, but non-summer time is still 08:15 ahead of the UTC time.

```
Ruijie(config)# clock timezone ABC 8 15
Set time zone name: ABC (GMT+08:15)
Ruijie(config)#show clock
16:39:16 ABC Wed, Feb 29, 2012
Ruijie(config)#show calendar
08:24:35 GMT Wed, Feb 29, 2012

Ruijie(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30 ahead 1 20
*May 10 03:45:58: %SYS-5-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday at 2:00
TO May the 3rd Monday at 18:30, ahead 1 hour 20 minute
Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at 18:30, ahead
1 hour 20 minute

Ruijie# show clock
18:00:08 TZA Wed, Feb 29, 2012

# If the time is set to non-summer time, the time zone name is restored to ABC.
Ruijie#clo set 18 1 1
*Jan 1 18:00:09: %SYS-5-CLOCKUPDATE: Set system clock: 18:00:09 ABC Sun, Jan 1, 2012
Set system clock: 18:00:09 ABC Sun, Jan 1, 2012
Ruijie#show clock
18:00:12 ABC Sun, Jan 1, 2012
```

If the system uses the default summer time that is one hour ahead of the standard time, ahead and the parameters behind ahead can be neglected. For example, set the summer time to start from 2:00 a.m. of the first Sunday in April to 2:00 a.m. of the last Sunday in October and set the summer time to one hour ahead of the standard time.

```
Ruijie(config)#clo summer-time PDT start April 1 sunday 2:00 end October last Sunday 2:00
*May 10 03:15:05: %SYS-5-CLOCKUPDATE: Set summer-time: PDT from April the 1st Sunday at 2:00 TO
October the last Sunday at 2:00, ahead 1 hour
Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at 2:00, ahead
1 hour
```

The following example disables summer time.

```
Ruijie(config)#no clock summer-time
*Jan 1 18:01:09: %SYS-5-CLOCKUPDATE: Set no summer time.
Set no summer time.
```

Check Method

-

Platform

-

Description


5.5 clock timezone

Use this command to set the time zone.

clock timezone [*name hours-offset* [*minutes-offset*]]

Use this command to remove the time zone settings.

no clock timezone

Parameter Description	Parameter	Description
	<i>name</i>	Time zone name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The name contains 3 to 31 characters.
	<i>hours-offset</i>	Hours of time difference. It indicates whether the time is faster or smaller than the hardware UTC time. The range is from -12 to 12. The negative digit indicates that the time is slower than the hardware time, while the positive digit indicates that the time is faster than the hardware time.  If the time is slower than the UTC time, add "-" before <i>hours-offset</i> .
	<i>minutes-offset</i>	Minutes of time difference. The range is from 0 to 59.

Defaults -

Command Mode Global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples The following example sets the time zone name to CST. The software time is 8 hours faster than the hardware time.

```
Ruijie(config)# clock timezone CST 8
Set time zone name: CST (GMT+08:00)

Ruijie# show clock
18:00:17 CST Wed, Dec 5, 2012
```

The following example sets the time zone name TZA. The software time is 06:13 slower than the hardware time.

```
Ruijie(config)# clock timezone TZA -6 13
Set time zone name: TZA (GMT-06:13)
```

The following example removes the time zone settings.

```
Ruijie(config)# no clock timezone
```

```
Set no clock timezone.
```

Check Method -

Platform -

Description -

5.6 clock update-calendar

Use this command to enable the system to synchronize the hardware time with the software time.

clock update-calendar

Parameter Description	Parameter	Description
	-	-

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported. After you configure this command, the system will synchronize the hardware time with the current software time according to the time zone and summer time settings of the device.

Configuration Examples The following example enables the system to synchronize the hardware time with the software time.

```
Ruijie# clock update-calendar
Set the hardware time from the system clock.
```

The following example sets the time zone of the hardware time to GMT+5:10, which indicates that the hardware time is 5:10 slower than the software time. The summer time is not set.

```
Ruijie# show clock
09:30:21 TSZ Wed, Feb 29, 2012

Ruijie# clock update-calendar
Set the hardware time from the system clock.

Ruijie#show calendar
04:20:25 UTC Wed, Feb 29, 2012
```

The following example sets the hardware time. If it is set to GMT+5:10 and the summer time is set to be 1:15 faster from the first Monday in February 1 to the second Sunday in June 1, it indicates that the

hardware time is 6:25 slower than the software time during the effective period of the summer time.

```
Ruijie# show clock
09:30:02 TSZ Wed, Feb 29, 2012

Ruijie# clock update-calendar
Set the hardware time from the system clock.

Ruijie#show calendar
03:05:08 UTC Wed, Feb 29, 2012
```

Check Method -

Platform -

Description

5.7 cpu high-watermark set

Use this command to set the high watermark of the CPU usage of the control core and enable CPU usage monitoring.

cpu high-watermark set [[**high** *high-value*] [**range** *range-value*]]

Use this command to disable CPU usage monitoring.

no cpu high-watermark set

Use this command to restore the default settings.

default cpu high-watermark set

Parameter Description	Parameter	Description
	high <i>high-value</i>	Sets the high watermark of the CPU usage. The range is from 2 to 99.
	range <i>range-value</i>	Sets the watermark fluctuation range. The range is from 1 to 20.
Defaults	By default, the watermark of the CPU usage is 80% and the watermark fluctuation range is 5% (namely, the range of the CPU usage watermark is from 75% and 85%).	
Command Mode	Global configuration mode	
Default Level	-	
Usage Guide	<p>This command is supported only in VSD0 mode. Multiple VSDs are not supported.</p> <p>You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.</p>	
Configuration Examples	<p>The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled).</p> <pre>Ruijie(config)# default cpu high-watermark set Reset default cpu watermark monitor set system cpu watermark high 80%(75~85%)</pre> <p>The following example disables CPU usage monitoring.</p> <pre>Ruijie(config)# no cpu high-watermark set Close cpu watermark monitor</pre> <p>The following example enables CPU usage monitoring. Keep the defined watermark value.</p> <pre>Ruijie(config)# cpu high-watermark set Open cpu watermark monitor set system cpu watermark high 80%(75~85%)</pre> <p>The following example enables CPU usage monitoring and sets the high watermark to 88% and fluctuation range to 3%.</p> <pre>Ruijie(config)# cpu high-watermark set high 88 range 3 Open cpu watermark monitor set system cpu watermark high 88%(85~91%)</pre> <p>In this case, the high watermark is set to 88%. The upper limit of the high watermark is 91% (88%+3%) and the lower limit is 85% (88%-3%).</p>	
Check Method	-	
Prompt Message	If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the following warning message when the CPU usage exceeds the upper limit of the high watermark:	

```
*Jan 19 16:23:01: %RG_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high watermark(85%),current cpu usage 100%
```

When the CPU usage is less than the lower limit of the high watermark, the system will print the following message about warning release:

```
*Jan 20 07:02:52: %RG_SYSMON-5- CPU_WATERMARK:withdraw warning! system cpu usage below high watermark(85%), current cpu usage 36%
```

Platform

-

Description

5.8 memory history clear

Use this command to clear the history of the memory usage.

memory history clear [one-fourth | half | all]

Parameter Description

Parameter	Description
one-fourth	Clears one fourth entries.
half	Clears a half of entries.
all	Clears all the entries.

Defaults

-

Command Mode

Global configuration mode

Default Level

-

Usage Guide

-

Configuration Examples

The following example clears a half of the history of the memory usage.

```
Ruijie# show memory history

Time Thu Jan 1 00:24:45 1970
Used(k) 148516
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      60600
rg_syslogd      36640

Time Thu Jan 1 00:24:41 1970
Used(k) 148492
Maxinum memory users for this period
```

```

Process Name      Holding
tcpip.elf         270028
cli-memory        52408
rg_syslogd        36640

Time Thu Jan  1 00:24:41 1970
Used(k) 148444
Maxinum memory users for this period
Process Name      Holding
tcpip.elf         270028
cli-memory        44088
rg_syslogd        36640

Ruijie(config)#memory history clear half
2 out of 5 records in the history table to be cleared...
Clear done !

```

Check Method -

Prompt -

Message -

Platform -

Description -

5.9 memory low-watermark set

Use this command to set the low watermark threshold of the memory and enable the memory low watermark detection.

memory low-watermark set *mem-set*

Use this command to disable the detection of memory low watermark.

no memory low-watermark set

**Parameter
Description**

Parameter	Description
<i>mem-rate</i>	Memory watermark threshold. The range is from 1% to 100%.

Defaults The default memory usage is 90%.

**Command
Mode** Global configuration mode

Default Level -

Usage Guide You can use this command to enable the detection of the memory low watermark and set the memory watermark threshold. When the system memory is less than this threshold, the system will print prompts.

Configuration The following example sets the low watermark threshold of the memory to 80%.

Examples Ruijie(config)#memory low-watermark set 80

Check Method -

Prompt When the system memory is less than the defined watermark value (such as 500000 KB), the system prints the following message:

Message

```
Ruijie(config)#<187> Jan 1 00:18:59 syslog: Free Memory has dropped below 500000k
```

Platform

Description -

5.10 reload

Use this command to reload the device.

reload [at { hour [:minute [:second]] } [month [day [year]]]

Parameter
Description

Parameter	Description
<i>hour</i> [: <i>minute</i> [: <i>second</i>]]	Sets the restart time in the format of hour : minute : second. Other neglected parameters keep the current system values.
<i>month</i>	Sets the month, in the range from 1 to 12.
<i>day</i>	Sets the day, in the range from 1 to 31.
<i>year</i>	Sets the year, in the range from 1970 to 2069.

Defaults -

Command Privileged EXEC mode
Mode

Default Level -

Usage Guide -

Configuration The following example reloads the device.

Examples

```
Ruijie# reload
Reload system?(Y/N) Y
Sending all processes the TERM signal... [ OK ]
Sending all processes the KILL signal... [ OK ]
Restarting system..
```


Check Method -

Prompt -
Message

Platform -
Description

5.11 show calendar

Use this command to display the hardware calendar.

show calendar

Parameter	Parameter	Description
Description	-	-

Command Privileged EXEC mode/ global configuration mode
Mode

Default Level -

Usage Guide -

Configuration The following example displays the hardware calendar.

Examples

```
Ruijie# show calendar
21:57:48 GMT Sun, Feb 28, 2012
```

Prompt -
Message

Platform -
Description

5.12 show clock

Use this command to display the system software clock.

show clock

Parameter	Parameter	Description
Description	-	-

Command Mode Privileged EXEC mode / global configuration mode

Default Level -

Usage Guide -

Configuration Examples The following example displays the software clock when the time zone is disabled.

```
Ruijie# show clock
18:22:20 UTC Tue, Dec 11, 2012
```

The following example displays the software clock when the time zone is enabled.

```
Ruijie# show clock
03:07:49 TSZ Wed, Feb 29, 2012
```

Prompt Message -

Platform Description -

5.13 show cpu

Use this command to display the information on the system task running on the control core instead of the non-virtual core.

show cpu

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported. If the system is equipped with a virtual core, you can use the **show processes cpu** command to check the CPU usage of the virtual core.

Configuration Examples The following example displays the information on the system task running on the control core instead of the non-virtual core.

```
Ruijie#show cpu
=====
```

```

CPU Using Rate Information
CPU utilization in five seconds:  4.80%
CPU utilization in one minute:    4.10%
CPU utilization in five minutes:  4.00%

NO      5Sec   1Min   5Min Process
  1    0.00% 0.00% 0.00% init
  2    0.00% 0.00% 0.00% kthreadd
  3    0.00% 0.00% 0.00% ksoftirqd/0
  4    0.00% 0.00% 0.00% events/0
--More--

```

Prompt -

Message -

Platform -

Description -

5.14 show memory

Use this command to display the system memory.

show memory [**sorted total** | **history** | **low-watermark** | *process-id* | *process-name*]

Parameter Description	Parameter	Description
	sorted total	Ranked according to the memory usage.
	history	Displays the history of memory usage.
	low-watermark	Displays the memory low watermark threshold of the system.
	<i>process-id</i>	Displays the memory usage of the task specified by <i>process-id</i> .
	<i>process-name</i>	Displays the memory usage of the task specified by <i>process-name</i> .

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide Every time when the **show memory history** command is used, the number of displayed entries increases by one. Up to 10 entries can be displayed. You can use the **memory history clear** command to clear history entries.

Configuration Examples The following example displays the memory usage of each task and the ranking (based on the total memory usage).

```
Ruijie# show memory sorted
```

```
System Memory: 508324K total, 481560K used, 26764K free, 31.5% used rate
Used detail: 149112K active, 247776K inactive, 30460K mapped, 50460K slab, 3752K others
```

PID	Text (K)	Rss (K)	Data (K)	Stack (K)	Total (K)	Process
807	1568	4584	264728	84	270028	tcpip.elf
854	40	1436	246076	84	248840	cli-filesystem
1237	52	1492	123260	84	126036	cli-memory
803	56	1104	74064	84	76920	ping.elf
727	84	1276	33812	84	36640	rg_syslogd
733	84	796	33536	84	36364	rg_syslogd
776	224	1416	16896	84	19800	lsmdemo
858	40	1324	16844	84	19612	rg-tty-admin
769	40	3600	11052	84	13812	skbdemo

```
--More--
```

Description of some keywords in the command:

Keyword	Description
total	Total system memory
used	Used memory
free	Remaining memory
used rate	Memory usage (percentage)
Active	Active page
inactive	Inactive page
mapped	Mapped memory
slab	Memory consumed by Slab
others	Memory capacity of the used memory except the memory used by active and inactive pages, mapped memory, and slab memory.

Description of the displayed information on each task:

Field	Description
PID	Process ID
Text	Code segment size
Rss	Resident memory size
Data	Data segment size
Stack	Stack size
Total	Total used memory
Process	Task name

Prompt

Message

Platform

Description

5.15 show memory vsd

Use this command to display memory information.

show memory vsd *vsd_id*

Parameter Description	Parameter	Description
	<i>vsd_id</i>	VSD ID is a digit. You can use the show vsd command to display the ID of each VSD. The ID range is from 0 to 16.

Command Privileged EXEC mode/ global configuration mode

Mode

Default Level -

Usage Guide

 This command is supported only in VSD0 mode.

Configuration

The following example displays the memory usage of each task in VSD 1 mode.

Examples

```
Ruijie#show memory vsd 1
PID      Text    Rss     Data    Stack   Total   Process
1408     244     1192    25400   84      32164   tty_secu_enable
1385     104     16288   648     84      18648   gvpd
1384     304     3872    17084   84      24728   wbamain
1382     376     17708   33656   84      53308   snooping.elf
1381     84      2156    16736   84      22956   password_policy
1380     72      1096    404     84      3848    dns_client.elf
1379     168     2580    472     84      5352    rg-rmond
1378     652     3504    9768    84      15964   rg-snmpd
1376     208     1452    10672   84      14872   rg-fsui
1375     116     2020    33464   84      37288   rg-telnetc
1373     24      844     220     84      2824    rg-telnetd
1372     724     2364    17016   84      24380   rg-sshd
1371     244     2996    35780   84      42544   rg-tty-admin
1365     132     2168    9004    84      13796   vrrp_plus.elf
1364     312     16944   764     84      20368   vrrp.elf
1363     124     16988   500     84      19744   lacp.elf
1358     24      1380    320     84      3536    ftpc_cli.elf
1357     124     1944    8552    84      14976   ftp_server.elf
1352     340     3032    74704   84      80768   dhcp6.elf
1351     312     1960    988     84      6116    dhcp.elf
1350     388     17808   920     84      21600   mstp.elf
1349     240     3876    976     84      9536    rpi.elf
1348     1316    4656    1004    84      10764   isis.elf
1347     212     4220    872     84      9368    ripng.elf
```

1345	460	4284	876	84	9656	rip.elf
1344	1800	5568	1572	84	12156	bgp.elf
1340	1084	4700	1024	84	10928	ldp.elf
1339	288	17684	556	84	21472	msf.elf
1338	208	3604	42712	84	47708	rg-syslogd
--More--						

Prompt
Message -

Platform
Description -

5.16 show pci-bus

Use this command to display the information on the device mounted to the PCI bus.

show pci-bus

Parameter	Parameter	Description
Description	-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Configuration Examples The following example displays the information on the device mounted to the PCI bus.

```
Ruijie# show pci-bus
NO:0
Vendor ID       : 0x1131
Device ID      : 0x1561
Domain:bus:dev.func : 0000:00:05.0
Status / Command : 0x2100000
Class / Revision : 0xc031030
Latency         : 0x0
first 64 bytes of configuration address space:
00: 31 11 61 15 00 00 10 02 30 10 03 0c 20 00 80 00
10: 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 61 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 01 2a

NO:1
Vendor ID       : 0x1131
Device ID      : 0x1562
Domain:bus:dev.func : 0000:00:05.1
Status / Command : 0x2100156
Class / Revision : 0xc032030
Latency         : 0x30
```

```
First 64 bytes of configuration address space:
00: 31 11 62 15 56 01 10 02 30 20 03 0c 20 30 80 00
10: 00 10 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 62 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 02 10
```

Prompt -
Message -
Platform -
Description -

5.17 show processes cpu

Use this command to display system task information.

show processes cpu [history [table] | [5sec | 1min | 5min | 15min] [nonzero]]

Parameter Description	Parameter	Description
	5sec 1min 5min 15min	Displays lists of tasks in descending order of CPU usage within the last five seconds, one minute, five minutes, and 15 minutes.
	Nonzero	Does not display the task with 0 CPU usage.
	History	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in histogram.
	Table	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in table.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples The following example displays the tasks listed in ascending order of task IDs.

```
Ruijie# show processes cpu
System Uptime: 19:08.6
CPU utilization for five seconds:1.2%; one minute:0.8%; five minutes:0.8%
set system cpu watermark (open): high 80%(85%~75%)

Tasks Statistics: 375 total, 10 running, 365 sleeping, 0 stopped, 0 zombie
  Pid Vsd S  PRI  P    5Sec    1Min    5Min    15Min Process
   1  0 S   20  0  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0)  init
   2  0 S   20  1  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0)  kthreadd
```



```

3  0 S  -100  0  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) migration/0
4  0 S   20  0  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) ksoftirqd/0
5  0 S  -100  1  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) migration/1

--More--

```

The following example displays the tasks listed in ascending order of task IDs without displaying the tasks with 0 CPU usage within 15 minutes.

```
Ruijie# show processes cpu nonzero
```

Description of the information displayed in this command:

Field	Description
System Uptime	Total running time of the device, precious to seconds.
CPU Utilization	Total CPU usage of the control core within the last five seconds, one minute, and five minutes.
Virtual CPU usage	Total CPU usage of the virtual control core within the last five seconds, one minute, and five minutes.
Tasks Statistics	Task statistics information, including the total number of statistics tasks and the task status.
set system cpu watermark	CPU watermark value and status of the control core.

The task running statuses are listed below:

Task Running Status	Description
running	Running task
sleeping	Suspended task
stopped	Stopped task
zombie	Terminated task, but not reclaimed by the system

Description of each task:

Field	Description
Pid	Task ID
Vsd	VSD ID
S	Task status. Five statuses in total: R (running), T (stopped), S (sleeping), D (waiting), and Z (zombie).
PRI	Task running priority
P	The core of the CPU on which the task runs
5sec/1min/5min/15min	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs.
Process	Task name. Only the first 15 characters are displayed. The remaining characters are truncated.


```

#-----#-----#-----*-->
0      50      100      second
system cpu percent usage(%) per 5second (last 125 second)
-----

system cpu percent usage(%) [last 60 minute]

-
100|
95 |
90 |
85 |
80 |
75 |
70 |
65 |
60 |
55 |
50 |
45 |
40 |
35 |
30|*
25||
20||
15||
10||
5 ||*
0 |||
#==*==>
0      minute
system cpu percent usage(%) per 1minute (last 2 minute)
-----

```

The following example displays the CPU usage of the core 0 in tables within the last 60 seconds, 60 minutes, and 72 hours.

The first table lists the CPU usage within 300 seconds. The first cell indicates the CPU usage within the last five seconds.

The second table lists the CPU usage within the last 60 minutes, measured in %. The two adjacent cells show the CPU usage measured at an interval of one minute.

The third table lists the CPU usage within the last 72 hours, measured in %. The two adjacent cells show the CPU usage measured at an interval of one hour.

Example:

```

Ruijie #show processes cpu history table
system cpu percent usage(%) [last 300 second]

```

```
#-----#
|      | 1| 2| 3| 4| 5| 6| 7| 8| 9| 10|
#-----#
#-----#
|      0| 2.0| 2.4| 2.3| 2.3| 2.8| 3.0| 2.7| 3.2| 2.6| 2.4|
#-----#
|      1| 2.7| 2.5| 2.7| 2.2| 2.4| 2.6| 2.2| 2.7| 2.3| 2.5|
#-----#
|      2| 2.9| 2.0| 2.4| 2.5| 2.7| 2.4| 2.4| 2.6| 2.6| 2.5|
#-----#
|      3| 2.7| 2.8| 2.8| 3.2| 2.5| 3.2| 3.1| 4.0| 2.7| 2.7|
#-----#
|      4| 4.0| 2.3| 2.1| 2.2| 2.7| 2.4| 2.5| 2.6| 2.4| 2.6|
#-----#
|      5| 2.4| 3.2| 2.5| 2.3| 2.3| 3.6| 2.8| 2.5| 2.2| 2.4|
#-----#

                system cpu percent usage(%) [last 60 minute]
#-----#
|      | 1| 2| 3| 4| 5| 6| 7| 8| 9| 10|
#-----#
#-----#
|      0| 2.6| 2.5| 3.0| 2.4| 2.6|
#-----#
```

Prompt -
Message
Platform -
Description

5.18 show processes cpu detailed

Use this command to display the details of the specified task.

show processes cpu detailed { *process-id* | *process-name* }

Parameter Description	Parameter	Description
	<i>process-id</i>	Displays the information on the task of the specified task ID.
	<i>process-name</i>	Displays the information on the task of the specified task name.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -


Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration The following example displays the information on the task of the specified task name.

Examples

```
Ruijie# show processes cpu detailed demo
Process Id   : 1820
Process Name : demo
Vsdid       : 0
Process Ppid : 1

State        : R(running)
On CPU       : 0
Priority      : 20
Age Time     : 24:06.5
Run Time     : 00:01.0
Cpu Usage    :
  Lass 5 sec  0.3% (0.6%)
  Lass 1 min  0.3% (0.6%)
  Lass 5 min  0.3% (0.6%)
  Lass 15 min 0.3% (0.6%)
Tty          : ?
```

 **Code Usage: 209.6 KB.** If the specified task name is not unique, the system displays the following message:

```
Ruijie# show processes cpu detailed demo
duplicate process, choose one by id not name.
name: demo, id: 1089, state: S(sleeping)
name: demo, id: 1091, state: R(running)
process name: monitor_procps, do NOT exist, or NOT only one.
```

Description of the displayed information:

Field	Description
Process Id	Task ID
Vsdid	VSD ID of the task
Process Name	Task name
Process Ppid	Parent process task ID
State	Task running status
On CPU	CPU where the task is running
Priority	Task priority
Age Time	Duration for the task from self-startup to now
Run Time	Duration for the task from self-startup to being executed

Cpu Usage	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs. For example, the demo task is running on No.0 core, which is the control core and the system has two control cores. In this case, the CPU usage is 0.3% (0.6%).
Tty	Tty ID, in the format of "Primary device ID, secondary device ID". If it is 0, the value is ?.
Code Usage	Size occupied by the task code segment

The following example displays the information on the task of the specified task ID.

```
Ruijie# show process cpu detailed 1715
```

Prompt Message -

Platform Description -

5.19 show processes vsd

Use this command to display system task of the specified VSD.

show process vsd vsd_id cpu

Parameter Description	Parameter	Description
	<i>vsd_id</i>	VSD ID is a digit. You can use the show vsd command to display the ID of each VSD. The range is from 0 to 16.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide  This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples The following example displays the system task information in VSD1 mode.

```
Ruijie#show processes vsd 1 cpu
```

Prompt Message -

Platform -
Description -

5.20 show reboot-reason

Use this command to display the reboot reason.

show reboot-reason

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode/ global configuration mode/ User EXEC mode

Default Level -

Usage Guide -

Configuration Examples The following example displays the reboot reason of the device.

```
Ruijie#show reboot-reason
time: 1970-01-01 08:03:13
reason: reload cmd
info: /sbin/rg-sysmon/3844

Ruijie#
```

Prompt Message -

Platform Description -

5.21 show usb-bus

Use this command to display the information on the device mounted to the USB bus.

show usb-bus

Parameter Description	Parameter	Description
	-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Configuration Examples 1: The following example displays the information on the device mounted to the USB bus.

```
Ruijie# show usb-bus
Device: Linux Foundation 2.0 root hub
Bus 001 Device 001: ID 1d6b:0002
```

Prompt Message -

Platform Description -

5.22 show version

Use this command to display the system version information.

show version

Parameter Description	Parameter	Description
	-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Usage Guide The following example displays the system version information.

```
Ruijie# show version
System description      : Ruijie Indoor AP320-I (802.11a/n and 802.11b/g/n) By Ruijie Networks
System start time      : 2012-12-06 00:00:00
System uptime          : 0:03:20:07
System hardware version : 1.0.0
System software version : AP_RGOS11.0(1B1)
System serial number    : 1234942570018
System boot version     : 1.0.0
```

Prompt -

Message

Platform

Description

-

6 Time Range Commands

6.1 absolute

Use this command to configure an absolute time range.

absolute { [**start** *time date*] [**end** *time date*] }

Use the **no** form of this command to remove the absolute time range.

no absolute

Parameter Description	Parameter	Description
	start <i>time date</i>	Indicates the start time of the range.
	end <i>time date</i>	Indicates the end time of the range.

Defaults No absolute time range is configured by default..

Command Mode Time range configuration mode

Default Level 14

Usage Guide Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.

Configuration Examples The following example creates a time range and enters time range configuration mode.

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

The following example configures an absolute time range.

```
Ruijie(config-time-range)# absolute start 1:1 1 JAN 2013 end 1:1 1 JAN 2014
```

Check Method Use the **show time-range** [*time-range-name*] command to display the time range configuration.

Prompt Message -

Platform Description -

6.2 periodic

Use this command to configure periodic time.

periodic *day-of-the-week time to [day-of-the-week] time*

Use the **no** form of this command to remove the configured periodic time.

no periodic *day-of-the-week time to [day-of-the-week] time*

Parameter Description	Parameter	Description
	<i>day-of-the-week</i>	Indicates the week day when the periodic time starts or ends.
	<i>time</i>	Indicates the exact time when the periodic time starts or ends.

Defaults No periodic time is configured by default.

Command Mode Time range configuration mode

Default Level 14

Usage Guide Use the **periodic** command to configure a periodic time interval to allow a certain function to take effect within the periodic time.

Configuration Examples The following example creates a time range and enters time range configuration mode.

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

The following example configures a periodic time interval.

```
Ruijie(config-time-range)# periodic Monday 1:1 to Tuesday 2:2
```

Check Method Use the **show time-range** [*time-range-name*] command to display the time range configuration.

Prompt Message -

Platform Description -

6.3 show time-range

Use this command to display the time range configuration.

show time-range [*time-range-name*]

Parameter	Parameter	Description
Description	<i>time-range-name</i>	Displays a specified time range.
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	Use this command to check the time range configuration.	
Configuration Examples	The following example displays the time range configuration.	
	<pre>Ruijie# show time-range time-range entry: test (inactive) absolute end 01:02 02 February 2012</pre>	
Prompt Message	-	
Platform Description	-	

6.4 time-range

Use this command to create a time range and enter time range configuration mode.

time-range *time-range-name*

Use the **no** form of this command to remove the configured time range.

no time-range *time-range-name*

Parameter	Parameter	Description
Description	<i>time-range-name</i>	Time range name
Defaults	No time range is configured by default.	
Command Mode	Global configuration mode	
Default Level	2	
Usage Guide	Some applications (such as ACL) may run based on time. For example, an ACL can be effective within	

certain time ranges of a week. To this end, first you must configure a time range. After the time range is created, you can configure relevant time control in time range mode.

Configuration The following example creates a time range.

Examples

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

Check Method Use the **show time-range** [*time-range-name*] command to display the time range configuration.

Prompt Message -

Platform Description -

7 HTTP Service Commands

7.1 enable service web-server

Use this command to enable the HTTP service function.

Use the **no** or **default** form of this command to disable the HTTP service function.

enable service web-server [**http** | **https** | **all**]

no enable service web-server [**http** | **https**]

default enable service web-server [**http** | **https**]

Parameter Description	Parameter	Description
	http	Enables the HTTP service.
	https	Enables the HTTPS service.
	all	Enables both the HTTP service and the HTTPS service.

Defaults By default, the HTTP service function is disabled.

Command mode Global configuration mode.

Usage Guide If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

Configuration The following example enables both the HTTP service and the HTTPS service:

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#enable service web-server
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.2 http port

Use this command to configure the HTTP port number.

Use the **no** form of this command to restore the default HTTP port number.

http port *port-number*

no http port

Parameter Description	Parameter	Description
	<i>port-number</i>	Configures the HTTP port number. The value includes 80, 1025 to 65,535.

Defaults The default HTTP port number is 80.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTP port number.

Configuration The following example configures the HTTP port number as 8080:

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#http port 8080
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.3 http secure-port

Use this command to configure the HTTPS port number.

Use the **no** form of this command to restore the default HTTPS port number.

http secure-port *port-number*

no http secure-port

Parameter Description	Parameter	Description
	<i>port-number</i>	Configures the HTTPS port number. The value includes 443, 1025 to 65,535.

Defaults The default HTTP port number is 443.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTPS port number.

Configuration The following example configures the HTTPS port number as 4443:

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#http secure-port 4443
```

**Related
Commands**

Command	Description
enable service web-server	Enables the HTTP service.
show web-server status	Displays the configuration and status of the Web service.

Platform N/A

Description

7.4 show web-server status

Use this command to display the configuration and status of the Web service.

show web-server status

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

**Command
mode** Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the configuration and status of the Web service:

Examples

```
Ruijie#show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
```

**Related
Commands**

Command	Description
enable service web-server	Enables the HTTP service.
http port	Configures the HTTP port number.

http secure-port	Configures the HTTPS port number.
-------------------------	-----------------------------------

Platform N/A

Description

7.5 upgrade web

Use this command to upgrade the Web package in local file system.

upgrade web *uri*

Parameter Description	Parameter	Description
	<i>uri</i>	The storage path of the Web package.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Please use the **copy** command to copy the Web package into the file system before you use this command to upgrade the Web package.

Configuration The following example copies a Web package into the file system and upgrades the package.

Examples

```
Ruijie#copy tftp://192.168.23.24/web.upd flash:/web.upd
Ruijie#upgrade web flash:/web.upd
```

Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.

Platform N/A

Description

7.6 upgrade web download

Use this command to download the Web package from the TFTP server and upgrade the package automatically.

upgrade web download { *oob_tftp: path* | *tftp: path* }

Parameter Description	Parameter	Description
	<i>oob_tftp: path</i>	<i>path</i> indicates the storage path of the Web package on the TFTP server.

	<p>oob_tftp indicates the system downloads the Web package from the TFTP server through the MGMT port and upgrades the Web package automatically.</p> <p>This parameter is supported only on the device supporting the MGMT port.</p>
tftp: path	<p><i>path</i> indicates the storage path of the Web package on the TFTP server.</p> <p>tftp indicates the system downloads the Web package from the TFTP server through the physical port and upgrades the Web package automatically.</p>

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example downloads a Web package form the TFTP server and upgrade the package automatically.

```
Ruijie#upgrade web download tftp://192.168.23.24/web.upd
```

Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.

Platform N/A

Description

7.7 webmaster level

Use this command to configure the username and password for Web login authentication. Use the **no** form of this command to restore the default setting.

webmaster level *privilege-level* **username** *name* **password** { *password* | [**0** | **7**] *encrypted-password* }

no webmaster level *privilege-level* [**username** *name*]

Parameter Description	Parameter	Description
	<i>privilege-level</i>	Configures the user privilege-level.
	<i>name</i>	Username.
	<i>password</i>	Password.
	0 7	Password type; 0 indicates plaintext, 7 indicates ciphertext.

<i>encrypted-password</i>	Password text.
---------------------------	----------------

Defaults

By default, two users are configured.

1. User1 is configured with privilege level 1, username of admin and plaintext password of admin.
2. User2 is configured with privilege level 2, username of guest and plaintext password of guest.

Command mode


Global configuration mode.

Usage Guide

When HTTP is enabled, users can log in to the Web interface only after being authenticated. Use this command to configure the username and password for Web login authentication.

Use the **no webmaster level** *privilege-level* command to delete all the usernames and passwords with a specified *privilege-level*.

Use the **no webmaster level** *privilege-level* **username** *name* command to delete the specified username and password.

 Usernames and passwords come with three permission levels, each of which includes at most 10 usernames and passwords.

Configuration

The following example configures the username and password for Web login authentication,

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#webmaster level 0 username ruijie password admin
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.

Platform

N/A

Description

8 Syslog Commands

8.1 clear logging

Use this command to clear the logs from the buffer in privileged EXEC mode.

clear logging

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.

Configuration The following example clears the log packets from the memory buffer.

Examples Ruijie# **clear logging**

Related Commands	Command	Function
	logging on	Turns on the log switch.
	show logging	Displays the logs in the buffer.
	logging buffered	Records the logs in the memory buffer.

Platform Description N/A

8.2 logging

Use this command to send the log message to the specified syslog server.

logging { *ip-address* | **ipv6** *ipv6-address* } [**udp-prot** *port*] [**vrf** *vrf-name*]

Use this command to delete the specified syslog server.

no logging { *ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* }

Use this command to restore the default port 514.

no logging { *ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* } **udp-prot**

Parameter	Parameter	Description
Description		

<i>ip-address</i>	Sets the IP address of the host receiving log messages.
<i>vrf-name</i>	Sets the VRF instance connecting with the host.
<i>ipv6-address</i>	Sets the IPv6 address of the host receiving log messages.
udp-port <i>port</i>	Sets the port number of the host receiving log messages. The default is 514.

Defaults No log message is sent to syslog server by default.

Command Global configuration mode

Mode

Usage Guide This command is used to configure a syslog server to receive log messages from the device. You can configure up to five syslog servers, log messages are sent to all configured syslog servers simultaneously,

Configuration The following example configures a syslog server with IP address 202.101.11.1.

Examples Ruijie(config)# logging 202.101.11.1

The following example configures a syslog server with IP address 10.1.1.100 and port number 8099.

Ruijie(config)# logging 202.101.11.1 udp-port 8099

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

Ruijie(config)# logging ipv6 AAAA:BBBB::FFFF

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

8.3 logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs at global configuration layer. Use the **no** form of the command to disable recording logs in the memory buffer. Use the **default** form of this command to restore the default setting.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

**Parameter
Description**

Parameter	Description
<i>buffer-size</i>	Size of the buffer is related to the specific device type: <ol style="list-style-type: none"> 1. For the kernel / aggregation switches, 4 K to 10 M bytes. 2. For the access switches, 4 K to 1 M Bytes. 3. For other devices, 4 K to 128 K Bytes.

<i>level</i>	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.
--------------	---

Defaults The buffer size is related to the specific device type.

1. kernel switches: 1 M Bytes;
2. aggregation switches: 256 K Bytes;
3. access switches: 128 K Bytes;
4. other devices: 4 K Bytes

The log severity is 7.

Command

Mode Global configuration mode

Usage Guide

The memory buffer for log is used in recycled manner. That is, when the memory buffer with the specified size is full, the oldest information will be overwritten. To show the log information in the memory buffer, run the **show logging** command in privileged user mode.

The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of the **clear logging** command in privileged user mode. To trace a problem, it is required to record logs in flash or send them to Syslog Server.


The log information is classified into the following 8 levels (Table 1):

Table-1

Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
informational	6	Descriptive information
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level.

When the level of log information to be displayed on devices is specified, the log information at or below the set level will be allowed to be displayed.

 After running the system for a long time, modifying the log buffer size especially in condition of large buffer may fails due to the insufficient available continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.

Configuration The following example allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes.

Examples

```
Ruijie(config)# logging buffered 10000 6
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays the logs in the buffer.
	clear logging	Clears the logs in the log buffer.

Platform N/A
Description

8.4 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the **no** form of this command to prohibit printing log messages on the console.

logging console [*level*]

no logging console

Parameter Description	Parameter	Description
	<i>level</i>	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 1.

Defaults The default is debugging (7).

Command Mode Global configuration mode

Usage Guide When a log severity is set, the log messages at or below that severity will be displayed on the console.

The **show logging** command displays the related setting parameters and statistics of the log.

Configuration The following example sets the severity of log that is allowed to be displayed on the console as 6:

Examples

```
Ruijie(config)# logging console informational
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays the logs and related log configuration parameters in the buffer.

Platform N/A

Description

8.5 logging count

Use this command to enable the log statistics function in global configuration mode. Use the **no** form of this command to restore the default setting.

logging count

no logging count

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The log statistics function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command enables the log statistics function. The statistics begins when the function is enabled. If you run the **no logging count** command, the statistics function is disabled and the statistics data is deleted.

Configuration Examples The following example enables the log statistics function:

```
Ruijie(config)# logging count
```

Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.6 logging facility

Use this command to configure the device value of the log information in global configuration mode. Use the **no** form of the command to restore the default setting.

logging facility *facility-type*

no logging facility

Parameter	Parameter	Description
Description	<i>facility-type</i>	Syslog device value. For specific settings, refer to the usage

guide.

Defaults The default is 23 if the RFC5424 format is enabled (Local7, local use).
The default is 16 if the RFC5424 format is disabled (Local0, local use).

Command Mode Global configuration mode

Usage Guide The following table (Table-2) is the possible device values of Syslog:

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization messages
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer subsystem
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization messages
11 (ftp)	FTP daemon
12 (ntp)	NTP subsystem
13 (logaudit)	log audit
14 (logalert)	log alert
15 (clock2)	clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

The default device value of RGOS is 23 (local 7).

Configuration The following example sets the device value of **Syslog** as **kernel**:

Examples Ruijie(config)# logging facility kern

Related Commands	Command	Description
	logging console	Sets the severity of logs that are allowed to be displayed on the console.

Platform Description N/A

8.7 logging file

Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH, USB or SD card. Use the no form of this command to restore the default setting,
logging file { flash:filename | usb0:filename | usb1:filename } [max-file-size] [level]
no logging file

Parameter Description	Parameter	Description
	flash	Saves the log file in expanded FLASH.
	usb0	Saves the log file in USB0. This parameter is supported by the device with one USB connector and the USB extension device.
	usb1	Saves the log file in the USB connector. This parameter is supported by the device with two USB connectors and the USB extension device.
	<i>filename</i>	Sets the file name. The file type is omitted, which is fixed as txt.
	<i>max-file-size</i>	Sets the maximum file size, in the range from 128K to 6M bytes, The default is 128K,
	<i>level</i>	Sets the level of the log message saved in the log file, which can be either the level name or the level number. The default is 6. See Usage Guide for details.

Defaults Log messages are not saved in expanded FLASH by default.

Command Mode Global configuration mode

Usage Guide You can save log messages in expanded FLASH if you don't want to transmit log messages on the network or there is no syslog server,
 The log file cannot be configured with the suffix, which is fixed as txt.

 If there is no expanded FLASH, the **logging file flash** command is hidden automatically and cannot be configured.

Keyword	Level	Description
---------	-------	-------------

Emergencies	0	Emergency case. The system fails to run.
Alerts	1	Problem that call for immediate solution.
Critical	2	Critical message.
Errors	3	Error message.
warnings	4	Alarm message.
Notifications	5	message that is normal but calls for attention.
informational	6	Descriptive message.
Debugging	7	Debugging message

Configuration Examples The following example saves the log message in expanded FLASH and sets file name, file size and log level to syslog.txt, 128K and 6 respectively.

```
Ruijie(config)# logging file flash:syslog
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.8 logging file numbers

Use this command to set the number of log files written into FLASH. Use the no form of this command to restore the default setting.

logging file numbers *numbers*

no logging file numbers

Parameter Description

Parameter	Description
<i>numbers</i>	Sets the number of log files written into FLASH, in the range from 2 to 32.

Defaults The default is 16.

Command Mode Global configuration mode

Usage Guide The system does not delete previously generated log files even if you change this configuration, Therefore, you need to delete the log files manually to save FLASH size (you can send log files to the

server through TFTP before that). For example, 16 log files are generated by default before you want to change the number to 2. New logs are overwritten constantly in log files indexed 0 to 1. However, log files indexed from 2 to 16 remain. You can delete these log files manually as needed.

Configuration The following example sets the number of log files written into FLASH to 8.

Examples Ruijie(config)# logging file numbers 8

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

8.9 logging filter direction

Use this command to filter the log messages destined to a certain direction. Use the no form of this command to restore the default setting.

logging filter direction { all | buffer | file | server | terminal }

no logging filter direction { all | buffer | file | server | terminal }

**Parameter
Description**

Parameter	Description
all	Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server.
buffer	Log messages destined to the log buffer are filtered, including log messages displayed by running the show logging command.
file	Log messages destined to the log file are filtered.
server	Log messages destined to the log server are filtered.
terminal	Log messages destined to the console and the VTY terminal (including Telnet and SSH).

Defaults

Log messages destined to all directions are filtered by default.

**Command
Mode**

Global configuration mode

Usage Guide

In general, log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. If you want to filter log messages destined to a certain direction, the terminal for instance, configure the terminal parameter.

**Configuration
Examples**

The following example filters log messages destined to the terminal (including the console and the VTY terminal).

Ruijie(config)# logging filter direction terminal

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

8.10 logging filter rule

Use this command to configure the filter rule of the log message,

logging filter rule { **exact-match** **module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*] }

Use this command to delete the “exact-match” filter rule.

no logging filter rule exact-match [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*]

Use this command to delete the “single-match” filter rule.

no logging filter rule single-match [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*]

Parameter Description	Parameter	Description
	exact-match	
single-match		Single-match filter rule. Fill in one of the following three parameters.
module <i>module-name</i>		Module name.
mnemonic <i>mnemonic-name</i>		Mnemonic name.
level <i>level</i>		Log level,

Defaults No filter rule is configured by default,

Command Mode Global configuration mode

Usage Guide If you want to filter a specific log message, use the “exact-match” filter rule and fill in all three parameters, namely, module name, mnemonic name and log level.
 If you want to filter a specific kind of log messages, use the “single-match” filter rule and fill in one of three parameters, namely, module name, mnemonic name and log level.
 When configured with the same module name, mnemonic name or log level, the “single-match” filter rule has a higher priority than the “exact-match” filter rule,

Configuration Examples The following example configures the “exact-match” filter rule with parameters of module name LOGIN, log level 5 and mnemonic name LOGOUT.

```
Ruijie(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5
```

The following example configures the “single-match” filter rule with the parameter of module name SYS.

```
Ruijie(config)# logging filter rule single-match module SYS
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

8.11 logging filter type

Use this command to configure the filter type of log messages. Use the no form of this command to restore the default setting.

logging filter type { contains-only | filter-only }

no logging filter type

Parameter Description

Parameter	Description
contains-only	The log message containing the key word of the filter rule is printed.
filter-only	The log message containing the key word of the filter rule is filtered.

Defaults


The default filter type is filter-only.

Command Mode

Global configuration mode

Usage Guide

1. When too many log messages are printed, the terminal screen keeps being refreshed. If you are not concerned with these log messages, use the “filter-only” filter type to filter the log messages,
2. If you are concerned with certain log messages, use the “contains-only” filter type to print log messages containing the key word of the filter rule, so as to monitor whether certain events happen.

 In real operation, the contains-only and the filter-only filter types cannot be configured at the same time.

 If you configure the filter direction and the filter type without configuring the filter rule, the log messages are not filtered.

Configuration The following example sets the filter type to contains-only.

Examples

```
Ruijie(config)# logging filter type contains-only
```

Related

Command	Description
---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

8.12 logging flash flush

Use this command to write log messages in the system buffer into the flash file immediately.


logging flash flush

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide In general, the log messages are cached in the log buffer. Only when the buffer is full or the timer expires are log messages written into the flash file. This command is used to write log messages in the system buffer into the flash file immediately.

 The **logging flash flush** command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.

Configuration Examples The following example writes log messages in the system buffer into the flash file immediately.

```
Ruijie(config)# logging flash flush
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

8.13 logging flash interval

Use this command to set the interval to write log messages into the flash file, Use the no form of this command to restore the default setting.

logging flash interval seconds


no logging flash interval

Parameter Description	Parameter	Description
	interval <i>seconds</i>	The interval to write log messages into the flash file, in the range from 1 to 57840 in the unit of seconds.

Defaults The default is 3600.

Command Mode Global configuration mode

Usage Guide This command is used to set the interval to write log messages into the flash file. The timer starts after configuration, If you want to restore the interval to 3600 seconds, use the **no logging flash interval** command.

 To avoid writing log messages into the flash file too frequently, it is not recommended to set a short interval.

Configuration The following example sets the interval to write log messages into the flash file to 300 seconds.

Examples Ruijie(config)# logging flash interval 300

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.14 logging life-time

Use this command to configure the preservation duration of logs in expanded FLASH. Use the no form of this command to restore the default setting.

logging life-time level *level days*

no logging life-time level *level*


Parameter Description	Parameter	Description
	<i>level</i>	Sets the log level, which can be either the level name or the level number.
	<i>days</i>	Sets the preservation duration of logs.

Defaults No preservation duration is set by default.

Command Global configuration mode

Mode

Usage Guide Due to difference in expanded FLASH size and log level, logs with different levels can be configured with different preservation durations.

 Once log preservation based on time is enabled, log preservation based on file size is disabled automatically. The log files are stored under the `syslog/` directory of the expanded FLASH,

Configuration The following example sets the preservation duration of logs whose level is 6 to 10 days.

Examples

```
Ruijie(config)# logging life-time level 6 10
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

8.15 logging monitor

Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.) in global configuration mode. Use the **no** form of this command to disable this function.

logging monitor [*level*]

no logging monitor

Parameter Description

Parameter	Description
<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table-1.

Defaults The default is debugging (7).

Command Mode

Global configuration mode

Usage Guide To print log information on the VTY window, run the **terminal monitor** command in privileged EXEC mode. The level of logs to be displayed is defined by **logging monitor**. The log level defined with "Logging monitor" is for all VTY windows.

Configuration The following example sets the severity of log that is allowed to be printed on the VTY window as 6:

Examples

```
Ruijie(config)# logging monitor informational
```

Related Commands	Command	Description
	logging on	
show logging		Displays the log messages and related log configuration parameters in the buffer.

Platform N/A
Description

8.16 logging on

Use this command globally to allow logs to be displayed on different devices. Use the **no** form of this command to disable this function.

logging on

no logging on

Parameter Description	Parameter	Description
	N/A	

Defaults Logs are allowed to be displayed on different devices.

Command Mode Global configuration mode

Usage Guide Log information can not only be shown in the Console window and VTY window, but also be recorded in different equipments such as the memory buffer, the expanded FLASH and the Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is greater than 1.

Configuration The following example disables the log switch on the device.

Examples

```
Ruijie(config)# no logging on
```

Related Commands	Command	Description
	logging buffered	
logging server		Sends logs to the Syslog server.
logging file flash:		Records logs on the expanded FLASH.
logging console		Allows the log level to be displayed on the console.
logging monitor		Allows the log level to be displayed on the VTY window (such as telnet window) .
logging trap		Sets the log level to be sent to the Syslog server.

Platform N/A
Description

8.17 logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. Use the **no** form of this command to disable this function.

logging rate-limit { *number* | **all** *number* | **console** { *number* | **all** *number* } } [**except** *severity*]

no logging rate-limit

Parameter	Parameter	Description
Description	<i>number</i>	The number of logs that can be processed in a second in the range from 1 to 10000.
	all	Sets rate limit to all the logs with severity level 0 to 7.
	console	Sets the amount of logs that can be shown in the console in a second.
	except	By default, the severity level is error (3). The rate of the log whose severity level is less than or equal to error (3) is not controlled.
	<i>severity</i>	Log severity level in the range from 0 to 7. The lower the level is, the higher the severity is.

Defaults The log rate limit function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to control the syslog output to prevent the massive log output.

Configuration Examples The following example sets the number of the logs (including debug) that can be processed in a second as 10. However, the logs with warning or higher severity level are not controlled:

```
Ruijie(config)#logging rate-limit all 10 except warnings
```

Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.18 logging rd on

Use this command in global configuration mode on the host to enable the log re-direction function and allow re-directing logs on slave or backup devices to the host in the VSU environment. Use **no** form of this command to disable this function.

logging rd on
no logging rd on

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The log re-direction function is enabled by default.

Command Mode Global configuration mode

Usage Guide The log information on slave or back devices not only can be shown on the Console window of slave or backup devices, but also can be re-directed to the host and exported to the Console and VTY windows of the host, and recorded in cache, expanded FLASH and Syslog Server of the host.

Configuration Examples The following example enables the log re-direction function on a device:

```
Ruijie(config)#logging rd on
```

Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.19 logging rd rate-limit

Use this command in global configuration mode on the host to enable the log re-direction rate limiting function to limit the number of logs that can be re-directed from a slave or backup device to the host each second in the VSU environment. Use the **no** form of this command to disable this function.

logging rd rate-limit *number* [**except** [*severity*]]
no logging rd rate-limit

Parameter	Parameter	Description
Description	<i>number</i>	Log information that can be re-directed each second, ranging from 1 to 10,000 logs
	except	Log information on or lower than the severity level will not be limited; error (3) by default, log information on or lower than

	the error level is not limited.
<i>severity</i>	Log information severity level; lower the level is, higher the severity is, ranging from 0 to 7

Defaults The maximum number of logs that can be re-directed each second is 200 by default.

Command Mode Global configuration mode

Usage Guide This command is used to control the output of log information by system re-direction. You can use this command to prevent a slave or backup device from re-directing a large number of logs to the host.

Configuration Examples The following example sets the maximum number of logs (including debug) that can be re-directed from a slave device to the host each second at 10, excepting logs on and above the warning severity level:

```
Ruijie(config)#logging rd rate-limit 10 except warnings
```

Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.20 logging server

Use this command to send the logs to the specified Syslog Sever in global configuration mode. Use the **no** form of this command to remove the setting. Use the **default** form of this command to restore the default setting.

logging server [**oob**] { *ip-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**udp-prot** *port*] [**vrf** *vrf-name*]

no logging server [**oob**] { *ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* } [**via** *mgmt-name*]

no logging server { *ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* } [**via** *mgmt-name*] **udp-prot**


Parameter Description	Parameter	Description
	oob	Specifies out-of-band communication for the logging server. (logs are sent through the MGMT port to the logging server.)
	<i>ip-address</i>	IP address of the host that receives log information.
	<i>vrf-name</i>	Specifies the VRF instance (VPN device forwarding table) connecting to the log host.
	<i>ipv6-address</i>	Specifies IPV6 address for the host receiving the logs.

via <i>mgmt-name</i>	Specifies the MGMT port for the oob option.
udp-port <i>port</i>	Specifies the port number for the specified host (The default port number is 514).

Defaults No log is sent to any syslog server by default.

Command Mode Global configuration mode

Usage Guide This command specifies a Syslog server to receive the logs of the device. Users are allowed to configure up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

 Only when the **oob** option is enabled can the **via** parameter be specified. Meanwhile, the **vrf** parameter cannot be set.

Configuration The following example specifies a syslog server of the address 202.101.11.1:

Examples Ruijie(config)# **logging server** 202.101.11.1

The following example specifies an ipv6 address as AAAA:BBBB:FFFF:

Ruijie(config)# **logging server ipv6** AAAA:BBBB:FFFF

Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays log messages and related log configuration parameters in the buffer.
	logging trap	Sets the level of logs allowed to be sent to Syslog server.

Platform Description N/A

8.21 logging source interface

Use this command to configure the source interface of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

logging source [**interface**] *interface-type interface-number*

no logging source [**interface**]

Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

Defaults No source interface is configured by default.

Command Mode Global configuration mode

Usage Guide By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses. If the source interface is not configured on the device, or no IP address is configured for the source interface, the source address of the log messages is the address of the sending interface.

Configuration The following example specifies loopback 0 as the source address of the syslog messages:

Examples Ruijie(config)# **logging source interface loopback 0**

Related Commands	Command	Description
	logging server	Sends logs to the Syslog server.

Platform Description N/A

8.22 logging source ip | ipv6

Use this command to configure the source IP address of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

logging source { **ip** *ip-address* | **ipv6** *ipv6-address* }

no logging source { **ip** | **ipv6** }

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the source IPV4 address sending the logs to IPV4 log server.
	<i>ipv6-address</i>	Specifies the source IPV6 address sending the logs to IPV6 log server.

Defaults No source address is configured by default.

Command Mode Global configuration mode

Usage Guide By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses. If this IP address is not configured on the

device, the source address of the log messages is the address of the sending interface.

Configuration The following example specifies 192.168.1.1 as the source address of the syslog messages:

Examples Ruijie(config)# **logging source ip** 192.168.1.1

Related Commands	Command	Description
	logging server	Sends the logs to the Syslog server.

Platform Description N/A

8.23 logging synchronous

Use this command to enable synchronization function between user input and log output in line configuration mode to prevent interruption when the user is keying in characters. Use the **no** form of this command to restore the default setting.

logging synchronous

no logging synchronous

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The synchronization function between user input and log output is disabled by default.

Command Mode Line configuration mode

Usage Guide This command enables synchronization function between user input and log output, preventing the user from interrupting when keying in the characters.

Configuration Ruijie(config)#**line console** 0

Examples Ruijie(config-line)#**logging synchronous**

Print UP-DOWN logs on the port when keying in the command, the input command will be output again:

```
Ruijie# configure terminal
```

```
Oct 9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down
```

```
Oct 9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to DOWN
```

```
Ruijie# configure terminal//----the input command by the user is output again rather than being intererupted.
```


Related Commands	Command	Description
	show running-config	Displays the configuration.

Platform Description N/A

8.24 logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server in global configuration mode. Use the **no** form of this command to prohibit sending log messages to the Syslog server.

logging trap [*level*]

no logging trap

Parameter Description	Parameter	Description
	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1.

Defaults The default is informational(6)

Command Mode Global configuration mode

Usage Guide To send logs to the Syslog Server, run the **logging** command in global configuration mode to configure the **Syslog Server**. Then, run the **logging trap** command to specify the severity level of logs to be sent.

The **show logging** command displays the configured related parameters and statistics of the log.

Configuration Examples The following example enables logs at severity 6 to be sent to the Syslog Server with the address of 202.101.11.22:

```
Ruijie(config)# logging 202.101.11.22
Ruijie(config)# logging trap informational
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	logging	Sends logs to the Syslog server.
	show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform Description N/A

8.25 logging userinfo

Use this command to enable the logging function to record user log/exit. Use the no form of this command to restore the default setting.

logging userinfo

no logging userinfo

Parameter Description	Parameter	Description
	N/A	N/A

Defaults No log message is printed recording user log/exit by default.

Command Mode Global configuration mode

Usage Guide This command is used to print the log message to remind the administrator of user login. The log message is in the format as follows:

```
Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68)
OK.
```

Configuration Examples The following example enables the logging function to record user log/exit.

```
Ruijie(config)# logging user-info
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.26 logging userinfo command-log

Use this command to enable the logging function to record user operation. Use the no form of this command to restore the default setting.

logging userinfo command-log

no logging userinfo command-log

Parameter Description	Parameter	Description
	N/A	N/A

Defaults No log message is printed recording user operation by default.

Command Global configuration mode

Mode

Usage Guide This command is used to print the log message to remind the administrator of configuration change. The log message is in the format as follows:

```
Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68)
command-log: logging server 192.168.23.68.
```

Configuration The following example enables the logging function to record user operation.

Examples Ruijie(config)# logging user-info command-log

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

8.27 service private-syslog

Use this command to set the syslog format to the private syslog format. Use the no form of this command to restore the default setting.

service private-syslog

no service private-syslog

Parameter Description

Parameter	Description
N/A	N/A

Defaults The syslog is displayed in the default format.

Command Global configuration mode

Mode

Usage Guide By default, the syslog is displayed in the format as follows:

```
*timestamp: %facility-severity-mnemonic: description
```

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

```
timestamp facility-severity-mnemonic: description
```

Here is an example:

```
May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console
```

The difference between the private syslog format and the default syslog format lies in the following

marks:

The private syslog does not have "*" before the timestamp, ":" after the timestamp and "%" before the identifying string.

Configuration The following example sets the private syslog format.

Examples Ruijie(config)# service private-syslog

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

8.28 service sequence-numbers

Use this command to attach serial numbers into the logs in global configuration mode. Use the **no** form of this command to restore the default setting.

service sequence-numbers

no service sequence-numbers

Parameter

Description

Parameter	Description
N/A	N/A

Defaults

No serial number is contained in the logs by default.

**Command
Mode**

Global configuration mode

Usage Guide

In addition to the timestamp, you can add serial numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.

Configuration The following example adds serial numbers to the logs.

Examples Ruijie(config)# **service sequence-numbers**

**Related
Commands**

Command	Description
logging on	Turns on the log switch.
service timestamps	Attaches timestamps to the logs.

Platform

Description

N/A

8.29 service standard-syslog

Use this command to set the syslog format to the standard syslog format defined in RFC3164. Use the **no** form of this command to restore the default setting.

service standard-syslog

no service standard-syslog

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The syslog is displayed in the default format.

Command Mode Global configuration mode

Usage Guide By default, the syslog is displayed in the format as follows:

*timestamp: %facility-severity-mnemonic: description

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

timestamp %facility-severity-mnemonic: description

Here is an example:

```
May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console
```

The difference between the standard syslog format and the default syslog format lies in the following marks:

The standard syslog does not have "*" before the timestamp and ":" after the timestamp.

Configuration The following example sets the standard syslog format.

Examples Ruijie(config)# service standard-syslog

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.30 service sysname

Use this command to attach system name to logs in global configuration mode. Use the **no** form of this command to restore the default setting.

service sysname

no service sysname

Parameter	Parameter	Description
Description	N/A	N/A

Defaults No system name is attached to logs by default.

Command Mode Global configuration mode

Usage Guide This command allows you to decide whether to add system name in the log information.

Configuration The following example adds a system name in the log information:

Examples

```

Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
Ruijie #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)#service sysname
Ruijie (config)#end
Ruijie #
Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console

```

Related Commands	Command	Function
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.31 service timestamps

Use this command to attach timestamp into logs in global configuration mode. Use the **no** form of this command to remove the timestamp from the logs. Use the **default** form of this command to restore the default setting.

service timestamps [*message-type* [**uptime** | **datetime** [**msec** | **year**]]]

no service timestamps [*message-type*]

default service timestamps [*message-type*]

Parameter	Parameter	Description
Description	<i>message-type</i>	The log type, including Log and Debug . The log type indicates the log information with severity levels of 0 to 6. The debug type indicates that with severity level 7.
	uptime	Device start time in the format of *Day*Hour*Minute*Second,

	for example, 07:00:10:41.
datetime	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07.
msec	Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299
year	Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07

Defaults The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.

Command Mode Global configuration mode

Usage Guide When the **uptime** option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the **datetime** option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.

Configuration Examples The following example enables the timestamp for **log** and **debug** information, in format of Datetime, supporting millisecond display.

```
Ruijie(config)# service timestamps debug datetime msec
Ruijie(config)# service timestamps log datetime msec
Ruijie(config)# end
Ruijie(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from console
by console
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	service sequence-numbers	Enables serial numbers of logs.

Platform Description N/A

8. 32 show logging

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from before to now.

show logging

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration Examples The following command displays the result of the **show logging** command with RFC5424 format disabled.

```
Ruijie# show logging
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to 202.101.11.22
    logging to 192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487: *Sep 19 02:46:13: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to down.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Ruijie %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to up.
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
```

Log information description:

Field	Description
-------	-------------

Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging** command with RFC5424 format enabled.

```
Ruijie# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
  logging to 192.168.23.89
  logging to 2000::1
  Delay-send logging: 2641 message lines logged
  logging to 192.168.23.89 by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address
```

```

for capwap.
<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881
name="" type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z ruijie SYS 6 SHELL_CMD
[USER@4881 name=""] [CMD@4881 task="rl_con" cmd="enable"]

```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

Related Commands

Command	Function
logging on	Turns on the log switch.
clear logging	Clears the log messages in the buffer.

Platform Description

N/A

8.33 show logging config

Use this command to display log configuration and statistics.

show logging config

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command

Privileged EXEC mode

Mode**Usage Guide** N/A**Configuration Examples** The following example displays the outcome of running the **show logging config** command with RFC5424 disabled.

```
Ruijie# show logging config
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to 202.101.11.22
    logging to 192.168.200.112
```

Field	Description
Syslog logging	Whether the logging function is enabled or disabled.
Console logging	The level and statistics of the log message printed on the console.
Monitor logging	The level and statistics of the log message printed on the VTY window.
Buffer logging	The level and statistics of the log message recorded in the memory buffer.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of debugging message.
Timestamp log messages	Timestamp format of log message.
Sequence-number log messages	Whether the sequence number function is enabled or disabled.
Sysname log messages	Adds the system name to the log message.
Count log messages	Log-counting function
Trap logging	The level and statistics of the log message sent to the syslog server.

The following example displays the outcome of running the **show logging config** command with RFC5424 enabled.

```
Ruijie# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
```

```

Statistic log messages: disable
Statistic log messages to terminal: disable
Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
Count log messages: enable
Trap logging: level informational, 2641 message lines logged,4155 fail
logging to 192.168.23.89
logging to 2000::1
Delay-send logging: 2641 message lines logged
logging to 192.168.23.89 by tftp
    
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to output console and remove terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending way and statistics

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.34 show logging count

Use this command to display the statistics about occurrence times, and the last occurrence time of each module log in the system in privileged mode.

show logging count

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode Privileged EXEC mode

Usage Guide To use the log packet statistics function, run the **logging count** command in global configuration mode. The **show logging count** command can show the information of a specific log, occurrence times, and the last occurrence time.
You can use the **show logging** command to check whether the log statistics function is enabled.

Configuration Examples The following example displays the result of the **show logging count** command:

```
Ruijie# show logging count
Module Name  Message Name  Sev  Occur      Last Time
SYS          CONFIG_I      5    1          Jul 6 10:29:57
SYS TOTAL                    1
```

Related Commands	Command	Function
	logging count	Enables the log statistics function.
	show logging	Displays basic configuration of log modules and log information in the buffer.
	clear logging	Clears the logs in the buffer.

Platform Description N/A

8.35 show logging reverse

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from now to before.

show logging reverse

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

Configuration The following command displays the result of the **show logging reverse** command with RFC5424

Examples

format disabled.

```

Ruijie# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to 202.101.11.22
    logging to 192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015491: *Sep 19 02:46:28: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to down.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015487: *Sep 19 02:46:13: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to up.

```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch

Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging reverse** command with RFC5424 format enabled.

```
Ruijie# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send
index:3, Cycle:10 seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
  logging to 192.168.23.89
  logging to 2000::1
  Delay-send logging: 2641 message lines logged
  logging to 192.168.23.89 by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<134>1 2013-07-24T12:29:34.343763Z ruijie SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:19:33.130290Z ruijie - 7 - - Please config the
IP address for capwap.
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.

Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

8.36 terminal monitor

Use this command to show logs on the current VTY window. Use the **no** form of this command to restore the default setting.

terminal monitor

terminal no monitor

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

Log information is not allowed to be displayed on the VTY window by default.

**Command
Mode**

Privileged EXEC mode

Usage Guide

This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is invalid. This command can be also executed on the console, but it does not take effect.

Configuration The following example allows log information to be printed on the current VTY window:

Examples

```
Ruijie# terminal monitor
```

Related

Command	Description
---------	-------------

Commands	N/A	N/A
-----------------	-----	-----

**Platform
Description** N/A

Command History	Version	Description
	N/A	N/A

9 CWMP Commands

9.1 acs password

Use this command to configure the ACS password to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to cancel the configuration.

acs password { *password* | *encryption-type encrypted-password* }



no acs password

Parameter Description	Parameter	Description
	<i>password</i>	Configures the ACS user password to be authenticated for the CPE to connect to the ACS.
	<i>encryption-type</i>	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
	<i>encrypted-password</i>	Specifies the password in encrypted form.

Defaults
 encryption-type: 0
 encrypted-password: N/A

Command Mode
 CWMP configuration mode

Usage Guide Use this command to configure the ACS user password to be authenticated for the CPE to connect to the ACS. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

-  The command contains English letters in upper or lower case and numeric characters.
-  Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples The following example configures the ACS password to be authenticated for the CPE to connect to the ACS to 123.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs password 123
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
------------------	---------	-------------

show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Platform N/A

Description

9.2 acs url

Use this command to configure the URL of the ACS to which the CPE will connect.

Use the **no** form of this command to restore the default setting.

acs url { *url* | **macc** }

no acs url

Parameter Description	Parameter	Description
	<i>url</i>	Specifies the URL of the ACS.
	macc	MACC

Defaults N/A

Command CWMP configuration mode

Mode

Usage Guide Use this command to configure the URL of the ACS to which the CPE will connect. If no ACS URL is manually specified but a dynamic ACS URL is obtained through DHCP, the CPE initiates a connection to the ACS using the dynamically obtained ACS URL. The URL of the ACS should meet the following format requirements:

- The URL of the ACS is formatted as [http://host\[:port\]/path](http://host[:port]/path) or [https://host\[:port\]/path](https://host[:port]/path).
- The URL of the ACS consists of at most 256 characters.

Use this command to connect to MACC. Running this command takes the same function as the following two commands:

- `acs url https://cloud.ruijie.com.cn/service/acs`
- `cpe inform interval 30`

Configuration The following example specifies the URL of the ACS to <http://10.10.10.1:8080/acs>.

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://10.10.10.1:8080/acs
Ruijie(config-cwmp)#
```

The following example specifies the URL of the ACS to `http://www.test.com/service/tr069servlet`.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://www.test.com/service/tr069servlet
Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.3 acs username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to restore the default setting.

```
acs username username
no acs username
```

Parameter Description

Parameter	Description
<i>username</i>	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Configuration Examples The following example configures the ACS username to be authenticated for the CPE to connect to the ACS to admin.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs username admin
Ruijie(config-cwmp)#
```

Related Commands

Command	Description
---------	-------------

show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs password	Configures the ACS password to be authenticated for the CPE to connect to the ACS.

Platform N/A

Description

cpe back-up

Use this command to configure the backup and restoration of the main program and configuration file of the CPE.

Use the **no** form of this command to disable this function.

cpe back-up [**delay-time** *seconds*]

no cpe back-up

**Parameter
Description**

Parameter	Description
<i>seconds</i>	Specifies the delay for backup and restoration of the main program and configuration file of the CPE, in the range from 30 to 10,000 in the unit of seconds

Defaults The default is 60 seconds.

Command CWMP configuration mode

Mode

Usage Guide

You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its main program or configuration file. Then when the CPE fails to connect to the ACS and breaks away from the NMS after its main program or configuration file is upgraded, the previous main program or configuration file of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong main program or configuration file.

Configuration Examples The following example disables the backup and restoration of the main program and configuration file of the CPE.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#no cpe back-up
Ruijie(config-cwmp)#
```

Related

Command	Description
---------	-------------

Commands	
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A

Description

9.4 cpe back-up

Use this command to enable the CPE backup function.

Use the **no** form of this command to restore the default setting.

cpe back-up [**delay-time** *seconds*]

no cpe back-up

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the backup delay time (30-10,000 seconds).

Defaults The default is 60 seconds.

Command CWMP configuration mode

Mode

Usage Guide After upgrading main programs or configurations, CPE cannot communicate with ACS for wrong configuration delivery. Use this command to recover the previous programs and configurations.

Configuration The following example disables the CPE backup function.

Examples

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#no cpe back-up
Ruijie(config-cwmp)#
```

Platform N/A

Description

9.5 cpe inform

Use this command to configure the periodic notification function of the CPE.

Use the **no** form of this command to restore the default setting

cpe inform [**interval** *seconds*] [**starttime** *time*]

no cpe inform


Parameter Description	Parameter	Description
	<i>seconds</i>	Specifies the periodical notification interval of the CPE in the range from 30 to 3,600 in the unit of seconds.
	<i>time</i>	Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.

Defaults The default is 600 seconds.

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the periodic notification function of the CPE.

- If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval.
- If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

 The narrower periodical notification interval allows the ACS to track the latest CPE status more accurately. However, narrower periodical notification interval brings about more sessions between the CPE and the ACS, consuming more resources of them. So the user should specify the periodical notification interval of the CPE to a reasonable value according to the network performance and the ACS performance.

Configuration Examples The following example specifies the periodical notification interval of the CPE to 60 seconds.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe inform interval 60
Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

9.6 cpe password

Use this command to configure the CPE password to be authenticated for the ACS to connect to the CPE. Use the **no** form of this command to cancel the configuration.

cpe password { *password* | *encryption-type encrypted-password* }



no cpe password

Parameter Description	Parameter	Description
	<i>password</i>	Configures the CPE user password to be authenticated for the ACS to connect to the CPE.
	<i>encryption-type</i>	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
	<i>encrypted-password</i>	Specifies the password in encrypted form.

Defaults
 encryption-type: 0
 encrypted-password: N/A

Command Mode
 CWMP configuration mode

Usage Guide
 Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

-  The command contains English letters in upper or lower case and numeric characters.
-  Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples
 The following example configures the CPE password to be authenticated for the ACS to connect to the CPE to 123.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe password 123
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

acs username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.
---------------------	--

Platform N/A
Description

9.7 cpe url

Use this command to configure the URL of the CPE to which the ACS will connect.
 Use the **no** form of this command to restore default setting.

cpe url *url*
no cpe url

Parameter Description	Parameter	Description
		<i>url</i>

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the URL of the CPE to which the ACS will connect. If no CPE URL is manually specified but a dynamic CPE URL is obtained through DHCP, the ACS initiates a connection to the CPE using the dynamically obtained CPE URL. The URL of the CPE should meet the following format requirements:

- The URL of the CPE is formatted as `http://ip [: port]/ path`.
- The URL of the CPE consists of at most 256 characters.

Configuration Examples The following example specifies the URL of the CPE to <http://10.10.10.1:7547/acs>.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe url Hhttp://10.10.10.1:7547/
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.8 cpe username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS.

Use the **no** form of this command to restore the default setting.

cpe username *username*

no cpe username

Parameter Description	Parameter	Description
	<i>username</i>	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Configuration Examples The following example configures the CPE username to be authenticated for the ACS to connect to the CPE to admin.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe username admin
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
	cpe password	Configures the CPE password to be authenticated for the ACS to connect to the CPE.

Platform N/A
Description

9.9 cwmp

Use this command to enable the CWMP function.

Use the **no** form of this command to disable this function.

cwmp

no cwmp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, this function is enabled.

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable the CWMP function.

Configuration Examples The following example disables the CWMP function.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#no cwmp
Ruijie(config)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

Platform N/A

Description

9.10 disable download

Use this command to disable the function of downloading main program and configuration files from the ACS. Use the **no** form of this command to restore the default setting.

disable download

no disable download

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the CPE can download main program and configuration files from the ACS.

Command Mode CWMP configuration mode

Usage Guide N/A

Configuration Examples The following example disables the function of downloading main program and configuration files from the ACS.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#disable download
Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

9.11 disable upload

Use this command to disable the function of uploading configuration and log files to the ACS.

Use the **no** form of this command to restore the default setting.

disable upload

no disable upload

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the CPE can upload its configuration and log files to the ACS.

Command Mode CWMP configuration mode

Usage Guide Disables the function of uploading configuration and log files to the ACS.

Configuration Examples The following example disables the function of uploading configuration and log file to the ACS.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Ruijie (config) #cwmp
Ruijie (config-cwmp) #disable upload
Ruijie (config-cwmp) #
```

**Related
Commands**

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.12 show cwmp configuration

Use this command to display the current configuration of CWMP.

show cwmp configuration

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

**Command
Mode** Privilege EXEC mode

Usage Guide

Configuration The following example displays the current configuration of CWMP.

Examples

```
Ruijie (config-cwmp) #show cwmp configuration
CWMP Status           : enable
ACS URL                : http://www.ruijie.com.cn/acs
ACS username          : admin
ACS password          : *****
CPE URL                : http://10.10.10.2:7547/
CPE username          : ruijie
CPE password          : *****
CPE inform status     : disable
CPE inform interval   : 60s
CPE inform start time : 0:0:0 0 0 0
CPE wait timeout      : 50s
CPE download status   : enable
CPE upload status     : enable
CPE back up status    : enable
```

```
CPE back up delay time      : 60s
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	Running status of CWMP.
ACS URL	URL of the ACS.
ACS username	ACS username to be authenticated for the CPE to connect to the ACS.
ACS password	ACS password to be authenticated for the CPE to connect to the ACS.
CPE URL	URL of the CPE.
CPE username	CPE username to be authenticated for the ACS to connect to the CPE.
CPE password	CPE password to be authenticated for the ACS to connect to the CPE.
CPE inform status	Status of CPE periodical notification function.
CPE inform interval	CPE periodical notification interval.
CPE wait timeout	Timeout period of CPE sessions.
CPE inform start time	The start time of periodical notification.
CPE download status	Indicates whether to download main program and configuration files from the ACS.
CPE upload status	Indicates whether to upload configuration files and log files to the ACS.
CPE back up status	Indicates whether backup and restoration of the main program and configuration file is enabled.
CPE back up delay time	Delay time of the backup and restoration of the main program and configuration files.

Related Commands

Command	Description
show cwmp status	Displays the running status of CWMP.

Platform N/A

Description

9.13 show cwmp status

Use this command to display the running status of CWMP

show cwmp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the running status of CWMP.

Examples

```
Ruijie#show cwmp status
CWMP Status           : enable
Session status        : Close
Last success session   : Unknown
Last success session time : Thu Jan 1 00:00:00 1970
Last fail session      : Unknown
Last fail session time : Thu Jan 1 00:00:00 1970
Session retry times    : 0
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	The running status of CWMP
Session status	The current status of the session between the CPE and the ACS
Last success session	The last success session type
Last success session time	The last success session time
Last fail session	The last failed session type
Last fail session time	The last failed session time
Session retry times	The number of session retransmission attempts

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.

Platform N/A

Description

9.14 timer cpe-timeout

Use this command to configure the session timeout period of the CPE.

timer cpe- timeout *seconds*

no timer cpe-timeout

Parameter Description

Parameter	Description
<i>seconds</i>	Sets the session timeout, in the range from 10 to 600 in the unit of

	seconds.
--	----------

Defaults By default, the session timeout period is 30 seconds.

Command CWMP configuration mode

Mode

Usage Guide Use this command to configure the session timeout period of the CPE.
The maximum waiting period that the CPE has when the CPE failed to receive the ACS reply.

Configuration The following example configures the session timeout period of the CPE to 50 seconds.

Examples

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#timer cpe-timeout 50
Ruijie(config-cwmp)#
```

**Related
Commands**

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A

Description

10 Monitoring Commands

10.1 fan mode

Use this command to configure the Operating Mode of Fans.

fan mode {normal | quiet | {defined [speed-level *level*]}}

Use the no form of this command to restore the default setting.

no fan mode

Use the **default** form of this command to restore the default setting.

default fan mode


Parameter Description	Parameter	Description
	normal	Indicates that the fans operate in standard mode (Normal Mode which is the default operating mode).
	quiet	Indicates that the fans operate in quiet mode (Quiet Mode).
	defined	Indicates that the fans operate in user-defined mode. (User Defined Mode) In user-defined mode, the rotating speed of each fan in the fan trays of the chassis is the same, which will not change as the system temperature changes. Therefore, the user-defined mode is not recommended.
	speed-level <i>level</i>	speed-level <i>level</i> : In user-defined mode, it specifies the rotating speed level of the fans. Seven levels are available; that is, the value of level ranges from 1 to 7. The rotating speed level is level 3 by default.

Defaults The default mode is **normal**.

Command Mode Global configuration mode

Level 14

Usage Guide Sets the fans to the normal mode, quiet mode or defined mode. After the operating mode of fans is configured, the starting speed of rotating is set under current temperature. The rotating speed of fans is automatically adjusted as the ambient temperature changes to achieve the best heat dissipation effect. In VSU mode, the fans in the two chassis operate in the same working mode.

-  The rotating speed of fans in user-defined mode is fixed. It can be set according to the level defined by users and will not automatically change as the temperature changes. Therefore, the standard mode or quiet mode is recommended so that the rotating speed of fans will automatically change as the temperature changes to protect the device from over-temperature which may cause

a fault of the device.

Configuration Fans operate in normal mode by default, and thus generate loud noise.

Examples

```
Ruijie(config)#fan mode quiet
```

When the ambient temperature is low, the user wants to adjust the rotating speed to the minimum to reduce noise to the most extent.

```
Ruijie(config)#fan mode defined speed-level 1
```

Verification Use the **show fan** command to display the operating mode of all the fan trays.

Use the **show fan detail** command to display the actual rotating speed of the internal small fans in each fan tray.

Prompt The quiet mode of fans is set successfully.

Messages

```
Fan mode has changed to user defined mode, with speed level 1.
```

The mode switching fails for the device error.

```
Failed to change fan mode, for device error.
```

Common

Errors If the ambient temperature changes greatly and you choose the user-defined mode, the rotating speed of the fans cannot be adjusted intelligently, causing a poor heat dissipation effect.



Platforms N/A

10.2 power cycle

Use this command to power off the specified board, and then power it on.

power cycle [**switch** *devid*] **slot** *slotid* [**interval** *seconds*]

Parameter Description	Parameter	Description
	switch <i>devid</i>	It is supported in VSU mode only. It specifies the chassis No. of the board to be powered on/off. By default, it refers to the current chassis.
	slot <i>slotid</i>	Specifies the slot No. of the board to be powered on/off. The supervisor modules are inserted in M1 and M2 slots. The FE cards are inserted in FE1, FE2, FE3, and FE4 slots.
	interval <i>seconds</i>	Specifies the time interval between power-off and the next power-on. The default interval is one second.

Command Mode	Privileged EXEC mode
Level	14
Usage Guide	<p>This command is used to power off the specified board, and then automatically power it on.</p> <ul style="list-style-type: none">  The hardware is equipped with the power-on protection function. When the board temperature exceeds 50C, the board does not power on immediately after the power-on operation is performed. The board will automatically power on after the board temperature drops below 50C. If the board temperature is already below 50C when the power-on operation is performed, the board powers on at once. Therefore, the actual power-on time may exceed the value of interval.  Do not manually power off the active supervisor module of the chassis. When the specified board is the active supervisor module of the chassis, the system prompts an error. In VSU mode, do not manually power off the local active supervisor modules in the two chassis.
Configuration Examples	<p>The following example shows slot 3 in the chassis is already upgraded and the upgrade result will be activated by using this command.</p> <pre>Ruijie#power cycle slot 3</pre> <p>The following example shows the FE card in slot 1 with over temperature needs to be powered off for 10 minutes and dissipated for heat and then be powered on for work.</p> <pre>Ruijie#power cycle slot FE1 interval 600 Slot FE1 power off successfully, and will be on beyond 600 seconds.</pre>
Prompt Messages	<p>The board is powered off successfully and will be powered on automatically after 5 seconds.</p> <pre>Slot 1/2 power off successfully, and will be on beyond 5 seconds.</pre> <p>The board is already powered off and will be powered on automatically after 5 seconds.</p> <pre>Slot 1/2 is already off, and will be on beyond 5 seconds.</pre> <p>The input slotid is not right.</p> <pre>Input slotid(L2) is error.</pre> <p>The device does not exist.</p> <pre>Device 2 does not exist.</pre> <p>The active supervisor module is not allowed to be manually power off.</p> <pre>Slot 1/M1 is master board, it cannot be control to power off.</pre> <p>The board does not exist.</p> <pre>Card in slot 1/2 is not inserted.</pre> <p>Operating mistakes cause power-on/off failure.</p> <pre>Failed to power cycle slot 1/2 for device error.</pre>

Platforms N/A

10.3 power on/off

Use this command to power on or off the specified board.



power {on | off} [switch *deviid*] slot *slotid*

Parameter Description	Parameter	Description
	on	Powers on the specified board.
	off	Powers off the specified board.
	switch <i>deviid</i>	It is supported in VSU mode only. It specifies the chassis No. of the specified board to be powered on/off. By default, it refers to the current chassis.
	slot <i>slotid</i>	Specifies the slot No. of the board to be powered on/off. The supervisor modules are inserted in M1 and M2 slots. The FE cards are inserted in FE1, FE2, FE3, and FE4 slots.

Command Mode Privileged EXEC mode

Level 14

Usage Guide This command is used to power on/off the specified board.

-  The hardware is equipped with the power-on protection function. When the board temperature is higher than 50C, the board cannot be powered on and the system prompts that power-on failed.
-  Do not manually power off the active supervisor module of the chassis. When the specified board is the active supervisor module of the chassis, the system prompts an error. In VSU mode, do not manually power off the local active supervisor modules in the two chassis.

Configuration The following example displays switch 2 slot 3 power-off.

Examples

```
Ruijie#power off switch 2 slot 3
Slot 2/3 power off successfully.
```

Prompt Messages The power-on is successful.

```
Slot 1/2 power on successfully.
```

The power-off is successful.

```
Slot 1/2 power off successfully.
```

The power is already on.

```
Slot 1/2 is already on.
```

The power is already off.

```
Slot 1/2 is already off.
```

The input slotid is not right.

```
Input slotid(L2) is error.
```

The device does not exist.

```
Device 2 does not exist.
```

The active supervisor module is not allowed to be manually power off.

```
Slot 1/M1 is master board, it cannot be control to power off.
```

The board does not exist.

```
Card in slot 1/2 is not inserted.
```

Over temperature on the current board cause power-on failure.

```
Failed to power on slot 1/2 for the card temperature is too high. Please try again later.
```

Operating mistakes cause power-on failure.

```
Failed to power on slot 1/2 for device error.
```

Operating mistakes cause power-off failure.

```
Failed to power off slot 1/2 for device error.
```

Platforms N/A

10.4 power priority

Use this command to set the power supply priority of a line card.

power priority [**switch** *devic*] **slot** *slotid* *prio*

Use this command to save the power-on priority.

power priority save

Use the **no** form of this command to restore the default priority with the power supply priority of a line card cancelled.

no power priority [**switch** *devic*] **slot** *slotid*

Use the **default** form of this command to restore the default setting. **default power priority** [**switch** *devic*] **slot** *slotid*

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
switch <i>devId</i>	It is supported in VSU mode only. Specifies the chassis No. of the board whose power-on/power-off priority is to be configured. By default, it refers to the current chassis.
slot <i>slotId</i>	Specifies the slot No. of the line card whose power-on/power-off priority is to be configured. Depending on the chassis type, a chassis may have 3 slots, 5 slots, 8 slots, or 12 slots.
<i>prio</i>	Specifies the line card priority to be set, ranging from 1 to 16, where 1 indicates the lowest priority and 16 the highest priority.
save	Saves the power-on priority

Defaults

By default, the power-on priorities are as following:

- The supervisor modules have the highest priority.
- The priority of an FE card is higher than the priority of the VSL card and other line cards.
- The priority of the VSL card is higher than the priorities of the other line cards.
- The smaller the slot number of a line card or FE card, the higher the priority of the line card or FE card.

By default, the line card is not automatically powered off based on the power supply priorities in the case of insufficient system power.

Command Mode

Global configuration mode

Level

14

Usage Guide

The power supply priorities of boards decide the power-on sequence of the boards. The higher the priority is, the earlier the power-on is. This command is used to change the default power supply priority of a line card or VSL card. The power supply priority of an FE card is defined by default, which cannot be changed.

Configuration Examples

The following example uses slot 3 as a back-up link with lower priority in VSU mode.

```
Ruijie(config)#power priority switch 2 slot 3 1
```

The following example configures slot 3 with the lowest priority in standalone mode which changes topology of networks and then adjust the priority to the highest.

```
Ruijie(config)#no power priority slot 3
Ruijie(config)#power priority slot 3 16
```

The following example introduces configuration files into the device in standalone mode and saves the power-on priority configuration of the line card.

```
Ruijie(config)#power priority save
```

Verification

Use the **show power priority** command to display the current power supply priorities of all line cards

and check whether the automatic power-off function is enabled on the line cards.

Prompt The device does not exist.

Messages Device 2 does not exist.

The board card does not exist.

Card in slot 1/2 is not inserted.

Operating mistakes cause priority configuring failure.

Failed to set slot 1/2 priority, for device error.

Common Errors N/A

Platforms N/A

10.5 show fan

Use this command to display the fan information in the slave chassis including the model number, serial number, operating status of every fan as well as the speed regulation pattern, actual rotating speed and other information.


show fan [{ [*devic*] *fanid*] **detail** } | **version**]

Parameter Description	Parameter	Description
	<i>devic</i>	It is supported in VSU mode only. When it specifies the display of detailed information about one single fan tray, it is used to specify their chassis number.
	<i>fanid</i>	Specifies the display of detailed information about fan tray ID. By default, it refers to full display. When one singled fan tray is specified in VSU mode, by default
	detail	Displays more detailed fan information. Displays the rotating speed of the internal small fans in each fan tray besides the displayed content by running the show fan command. Displays detailed failure information if the fan is in failure. Detailed information of all fan trays is enabled by default. When it specifies fan tray ID, only the detailed information of the corresponding fan tray is displayed.
	version	Displays the fan version.

Command Mode Privileged EXEC mode

Level 14

Usage Guide Use the **show fan** command to display the fan information about fans in the slave chassis. Use the **show fan** command without parameters to display the module number, serial number, operating status and speed adjustment mode of all the fan trays.

-  Use the show fan detail command to further displays detailed failure causes when the fan stray is in failure.

Configuration The following example displays the fan information in S8605E slave chassis.

Examples

```
Ruijie#show fan
Chassis-type: RG_S8605E
Fan-id: 1
  Fan-type:      M05_FAN
  Serial Number: 1234567890123
  Energy-saving: off

fan-id  status  mode      speed-level
-----  -
1       ok       normal    N/A
```

The following example displays the detailed fan information.

```
Ruijie#show fan detail
Chassis-type: RG_S8605E
Fan-id: 1
  Fan-type:      M05_FAN
  Serial Number: 1234567890123
  Energy-saving: off
  Status:        ok
  Mode:          normal

sub-fan-id  status  speed
-----  -
1           ok      2700
2           ok      3000
3           ok      3000
4           ok      3150
5           ok      2850
6           ok      3000
7           ok      3000
8           ok      3150
```

The following example displays only the detailed information about Fan 1.

```
Ruijie#show fan 1 detail
Chassis-type: RG_S8605E
Fan-id: 1
```



```

Fan-type:      M05_FAN
Serial Number: 1234567890123
Energy-saving: off
Status:       ok
Mode:        normal

```

```

sub-fan-id  status  speed
-----  -
1           ok      2850
2           ok      3000
3           ok      3000
4           ok      3150
5           ok      3000
6           ok      3000
7           ok      3000
8           ok      3000

```

Prompt Messages N/A

Platforms N/A

10.6 show power

Use this command to display power information including that of its basic condition, power allocation and version and etc.

show power [priority | version]

Parameter Description	Parameter	Description
	priority	Displays the power supply priority configuration of all boards and checks whether the automatic power-off function is enabled.
	version	Displays the serial number, hardware and software version as well as other information about each power.

Command Mode Privileged EXEC mode

Level 14

Usage Guide This command is used to display power information about the slave chassis, and the command without parameters is used to display the most fundamental power information including:

- Display the model, on-off status, rated and out power, output current, input and output voltage, Fail/ alarm status (specific to input overvoltage / undervoltage alarm, output overvoltage/undervoltage

alarm, temperature alarm, fan failure alarm and over-temperature alarm and etc.) of each power on every slot.

- Display the system's total power, allocated and occupied power and available power.
- Display the name, demanded power and allocated power of each board on every slot and power supply status of each slot.

Configuration The following example displays the basic power information.

Examples

```
Ruijie#show power
Chassis-type: RG_S8605E
Power-redun: no
Energy-saving: off
power-id power-type supply(W) status vol-in/out(V) cur-out(mA)
supply-out(W)
-----
-----
1 PA600I 600 ok 231 /12 3500 42
2 PA600I 600 ok 232 /12 1000 12
3 PA1600I_P 1600 ok N/A /55 0 0

slot card_type status require(W) allocate(W)
-----
-----
1 N/A N/A N/A N/A
2 M18000-48GT-CB power-off 349 0
3 N/A N/A N/A N/A
M1 M18010-CM power-on 40 40
M2 M18010-CM power-on 40 40

system_supply(W) card_allocate(W) fan_allocate(W) free_supply(W)
-----
-----
1200 80 288 832
```

The following example displays the power version.

```
Ruijie#show power version
Chassis-type: RG_S8605E
Power-id: 1
Serial Number: ZH40274
Type: PA600I
Hardware Version: 1
Software Version: N/A
Temperature(C): 44
Power-id: 2
Serial Number: ZJ47958
Type: PA600I
```

```

Hardware Version: 2
Software Version: N/A
Temperature (C): 44
Power-id: 3
Serial Number: LBLNPW12CS33014774
Type: PA1600I_P
Hardware Version: N/A
Software Version: N/A
Temperature (C): 37

```

The following example displays the power supply priority of the board.

```

Ruijie#show power priority
Chassis-type: RG_S8605E
Card Auto-down: off

slot  priority  status
-----  -
1      N/A      N/A
2      1        power-off
3      N/A      N/A
M1     N/A      power-on
M2     N/A      power-on

```

Prompt Messages N/A

Platforms N/A

10.7 show temperature

Use this command to display board temperature, threshold configuration and other information.

show temperature

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode

Level 14

Usage Guide Use the command to display the current temperature and threshold configuration of each board. The temperature threshold of CA products involves the alarm threshold and the hazard threshold.

Alarm threshold: When the temperature of the board exceeds the alarm threshold, the active supervisor module generates a Syslog message and the Alarm LED on the panel becomes yellow.

Hazard threshold: It indicates the power-off temperature. When the temperature of the board exceeds the hazard threshold, the board powers off automatically. In addition, the active supervisor module generates a Syslog message and the Alarm LED on the panel becomes red.


Configuration The following example displays the temperature and threshold configuration of all boards.

Examples

```
Ruijie#show temperature
Chassis-type: RG_S8605E
slot   card_type           warning (C)  shutdown (C)  current (C)
-----
-----
1      N/A                   N/A         N/A           N/A
2      M18000-48GT-CB         51          90 |100 |100  26|27|32|33| (N/A) | (N/A)
3      M18000-10QXS-CB       51          90 |100 |100  24|26|28|30| (35) | (64)
M1     M18010-CM              51          90 |100 |100  24|29|26|29| (35) | (N/A)
M2     M18010-CM              51          90 |100 |100  23|29|25|29| (34) | (N/A)
```

Field Description

Field	Description
Chassis-type	Type of the chassis
slot_id	Slot No. of the chassis
card_type	Type of the board in corresponding position and "N/A" represents no board plugged into the slot.
warning	Board alarm temperature (in degree Celsius) only includes the alarm threshold of the main board temperature (that of air inlet, air outlet and hottest pints on the board).
shutdown	The hazard threshold of the board, that is, the power-off threshold (in degree Celsius) . Three types of power-off threshold are listed as following : the main board temperature , CPU temperature, and MAC temperature.
current	Displays current board temperature. Displays "N/A" if the temperature cannot be gained. The temperatures from left to right are that of the following: air inlet, air outlet, and the hottest points (two on each board), CPU (two multi-service cards), and MAC ("N/A is displayed when the engine does not involve MAC. Some cards have several MAC temperature).

 When the main supervisor module is used to control all the modules, it will not automatically power off when its temperature reaches the hazard threshold. It's recommended to take actions for heat

dissipation by users.

Prompt Messages N/A

Platforms N/A

10.8 threshold set temperature

Use this command to set the temperature threshold for the board.

threshold set temperature [switch *devic*] {board | cpu | mac} {warning | shutdown} *temp*

Use the **no** form of this command to restore the default setting.

no threshold set temperature

Use the **default** form of this command to restore the default setting.

default threshold set temperature

Parameter Description

Parameter	Description
switch <i>devic</i>	It is supported in VSU mode only. It specifies the chassis No. of the board whose temperature thresholds are to be configured. By default, it refers to the current switch.
board	Specifies the temperature thresholds of the main board, including the temperatures of the air inlet, air outlet, and the hottest points on the main board. The temperature thresholds of the main boards are the same for all the boards.
cpu	Specifies the CPU temperature thresholds. The CPU temperature thresholds are the same for all the boards.
mac	Specifies the MAC temperature thresholds. The MAC temperature thresholds are the same for all the boards.
warning	Specifies the alarm threshold of the board temperature. When the temperature detection point is cpu or mac, this key word is invisible.
shutdown	Specifies the hazard threshold (that is, the power-off threshold) of the board temperature.
<i>temp</i>	Specifies the temperature threshold.

Defaults

Only the main board temperature involves both an alarm threshold and a hazard threshold.


The alarm threshold of the main board temperature is 56C and the hazard threshold is 80C; the hazard threshold of the CPU and MAC temperatures is 100C, and the CPU and MAC temperatures do not involve any alarm threshold by default.

Command

Global configuration mode

Mode**Level** 14

Usage Guide Use the `show temperature` command to check the alarm and hazard thresholds of the current board. The alarm threshold of the main board temperature is 56C and the hazard threshold is 80C; the hazard threshold of the CPU and MAC temperatures is 100C, and the CPU and MAC temperatures do not involve any alarm threshold by default. The `no` form of this command is used to remove the hazard thresholds of all boards. In VSU mode, the thresholds of two chassis will be both removed and restored to the default setting.

 The hazard threshold of the main board temperature cannot exceed 90C. The hazard thresholds of the CPU and MAC temperatures cannot exceed 110C.

 The hazard thresholds of the CPU and MAC temperatures cannot exceed 110C.

Configuration Examples The following example configures the warning threshold of the main board as 75°C to stop high-temperature alerts .

```
Ruijie(config)#threshold set temperature board warning 75
```

The following example configures the temperature alarm threshold of the main board in the two chassis as 75°C in VSU mode.

```
Ruijie(config)#threshold set temperature switch 1 board warning 75
```

```
Ruijie(config)#threshold set temperature switch 2 board warning 75
```

Verification Use the **show temperature** command to display the alarm and hazard thresholds of the current board.

Prompt Messages The device does not exist.

```
Device 2 does not exist.
```

2. The alarm threshold set is higher than the hazard threshold.

```
The warning temperature must be less than the shutdown temperature(80).
```

Operating mistakes cause temperature threshold configuration failure.

```
Failed to set temperature threshold, for device error.
```

Common Errors 1. When the thresholds exceed the allowed values, the threshold settings are invalid.
2. When the alarm thresholds are excessively low, the system frequently generates alarm logs.

Platforms N/A

11 LICENSING Commands

11.1 license copy

Use this command to back up a license file.

license { **copy-all** | **copy-file** *filename* } { **flash:** | **usb0:** } [*target-filename*]

Parameter description	Parameter	Description
	copy-all	Copies all permanent license files in the system.
	copy-file	Copies the <i>filename</i> license file in the system. And filename can be the name of a license file already installed in the system or the name of a feature. When filename is a feature name, all license files already installed for this feature are backed up.
	<i>filename</i>	The name of a license file already installed in the system or the name of a feature
	flash:	Specifies that the license file is installed in the internal flash file system.
	usb0:	Specifies that the license file is installed in the USB file system.
	<i>target-filename</i>	Specifies the name of the license file.

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide When you back up all license files in the system, a tar file is generated. This command does not require authorization.
Both one license file and all license files of a certain feature can be copied.

Configuration Examples The following example backs up all license files in the system into file-rg-license-lics in a USB flash drive (there must be this path) and name the backup lics.tar.

```
Ruijie#lic copy-all usb0:rg-license-lics/lics.tar
Success to copy all permanent license.
```

Verification You can run the **dir** command to check whether the license file backup is generated. In addition, you can check whether the backup is correct by comparing the output of the **dir** command with the license file name in the **installed license** field of the feature with permanent authorization displayed by running the **show license all_license** command.

 Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance

license file exists in the system at a time; therefore, the single-instance license file backup is named after the feature.

i In this example, the IDs 19881021.lic and 19881023.lic are embedded in the license file. License files are stored in different folders based on the features during the packing; therefore, users can still identify the mapping between license files and features.

Prompt There is not permanent license in the system for backup.

Messages Copy failed, there's no permanent license in the system.

All license files in the system are successfully backed up.
Success to copy all permanent license.

The error message is displayed if no feature or license file is specified on the device.
Copy failed, there's no such service or license installed in the system.

The error message is displayed if the specified license file is temporary.
Copy failed, the license is temporary.

The specified license file is backed up successfully.
Success to copy license vsd.lic.

Common Specify a license file or a file not in the system.

Errors Specify a temporary license file for backup (a temporary license file cannot be backed up).

11.2 license grace-period

Use this command to set the time of issuing a warning before the validity period of a license file expires. Use the **no** or **default** form of this command to restore the default setting.

license grace-period *license days*
no license grace-period *filename*
default license grace-period *filename*

Parameter Description	Parameter	Description
	<i>filename</i>	The name of the license file for a feature
	<i>days</i>	The period from the expiry time to the warning time


Defaults The default value is the smaller one between 120 and half the evaluation license file's validity period.

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide When the timeout interval of a license file is shorter than the friendly period, the friendly period warning is generated once a day; and the warning is generated once an hour one day before the license file expires. Friendly period warning is issued in log or SNMP TRAP form.

 This command does not require authorization.

 An evaluation license file needs to be configured with friendly period warning. A permanent license file does not need to be configured with friendly period warning.

Configuration Examples The following example shows that the temporary license file for the VSD feature has already been installed on the device, and the friendly period warning time is set to 100 days.

```
Ruijie#license grace-period LIC-VSD 100
Success to set alarm starting point of license LIC-VSD.
```

Verification When the validity period of the license file for the VSD feature is shorter than 100 days, the friendly period warning is displayed at regular intervals.

Prompt The setting is successful.

Messages Success to set alarm starting point of license LIC-VSD.

The specified license file is not in the system.

There's no license abc in the system.

Common Errors Specify a license file not in the system.

11.3 license install

Use this command to install a license file.

license install { **flash:** | **usb0:** } *filename*

Parameter Description	Parameter	Description
	flash:	Specifies that the license file is installed in the internal flash file system.
	usb0:	Specifies that the license file is installed in the USB file system.
	<i>filename</i>	Specifies the name of the license file.

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide The name of the license file can be modified. This command does not require authorization.

Configuration The following example obtains the host ID of the device, registers at the authorization website, obtains and installs the license file of the VSD function.

Examples

```
Ruijie#show license hostid
8708EH5F00042
Ruijie#license install usb0:vsd.lic
License file install success, service name: LIC-VSD.
```

Verification Run the **show license all_license** command to check the license name. If the license name is displayed, the corresponding license file is installed.

Prompt

The specified license file is not in the system.

Messages

```
Install failed: no such file or directory.
```

The specified license file is not legal.

```
Install failed: the install license may be wrong.
```

The specified license file is newer than the installed one.

```
Install failed: the system already has a same license which is newer.
```

The license file is reinstalled.

```
Install failed: the license has been installed before.
```

The specified license file is temporary and there is the same permanent one.

```
Install failed: The system already has a same permanent license.
```

The license file is installed successfully (use the license file for VSD as an example).

```
License file install success, service name: LIC-VSD.
```

The license file is installed successfully and becomes permanent (use the license file for VSD as an example).

```
License file install success, service name: LIC-VSD.
```

```
The license turns to be permanent.
```

The license file is installed successfully whose expiry date is close (use the license file for VSD as an example).

```
License file install success, service name: LIC-VSD.;
```

```
The installed license is approaching deadline, less than 30 days.
```

Common

Specify a license file not on the device.

Errors

Specify a license file illegal.

Specify a license file to install older than existing one in the system.

Reinstall the license file.

Replace the permanent license file with the temporary license file.

11.4 license unbind

Use this command to unbind a license.


license unbind *pak*


Parameter Description	Parameter	Description
	<i>pak</i>	The license code

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide This command does not require the license.

 Use this command to unbind a license from the bound device before performing unbinding on the Web page.

 You will get an authenticocode after unbinding the license from the device, which is necessary for unbinding operation on the Web page.

Configuration Examples The following example unbinds license code LIC-FCOE00000012268888.

```
Ruijie#license unbind LIC-FCOE00000012268888
Success to unbind license LIC-FCOE00000012268888.
The verification string is
775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355
855.
```

11.5 license uninstall

Use this command to remove a license file.


license uninstall { **all** | *license* [*filename*] }


Parameter Description	Parameter	Description
	all	Removes all license files in the system.
	<i>license</i>	The name of the license to be removed
	<i>filename</i>	The name of the file to be removed

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide This command does not require authorization.

 After you remove the license file for a feature that is running, the license file removal does not take effect immediately.

 A license file cannot be restored after it is removed. It is recommended that you back up the license file before removing it.

Configuration The following example removes the license file for VSD in the system.

Examples

```
Ruijie#license uninstall LIC-VSD
Uninstall LIC-VSD success.
```

Verification Run the **show license all_license** command to view the **Service name** filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Prompt The specified license file is not on the device. (it is named after defd in this example).

Messages

```
Uninstall failed: there's no license defd in the system.
```

The specified license file of the specified feature is not on the device (The specified feature is LIC-WLAN-AP-32 and the specified license is named 123.lic).

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in the
system.
```

The single instance license does not support license based uninstalling.

```
Uninstall failed: single instance license does not support license based
uninstalling.
```

The removing is successful (use VSD feature as an example).

```
Uninstall LIC-VSD success.
```

The removing of a license file is successful (LIC-WLAN-AP-32 is the name of the specified file and AP32_1.lic is a license file in this example).

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 success.
```

Common The license file has not been installed on the device.

Errors Specify a license file not on the device.

Remove a certain license file for a single-instance feature (One single-instance license does not support the removing of one single file).

11.6 license update

Use this command to update a license file.

license update { **flash:** | **usb0:** } *filename*

Parameter Description	Parameter	Description
	flash:	Specifies that the license file is installed in the internal flash file system.
	usb0:	Specifies that the license file is installed in the USB file system.
	<i>filename</i>	Specifies the name of the license file.

Command Mode Privileged EXEC mode

Default Level 4

Usage Guide This command does not require authorization. The name of a license file can be modified.

Configuration Examples The following example updates the temporary license file for VSD in the system to a permanent license file.

- Purchase the permanent license file `vsd_perm.lic` for VSD, store the `vsd_perm.lic` file in a USB flash drive, and connect the USB flash drive to the device.
- Update the license file for VSD.

```
Ruijie#license update usb0:vsd_perm.lic
License file update success, temporary license LIC-VSD changes into permanent.
```

Verification Run the **show license** command to check the **Attribute** field. If the field is displayed as Permanent, the corresponding attribute is updated.

```
Ruijie #show license all-license
Searching license in the system...
  1. Service name: LIC-VSD
Attribute: Permanent, Multiple instance, Releasable
Installed licenses(s): 123.lic
```

Prompt The specified license file is not in the system.

Messages Update failed: No such file or directory.

The specified license file is not legal.

Update failed: the update license may be wrong.

The specified license file is newer than the installed one.

Update failed: the new installed license is older than the system one.

The license file is reinstalled.

Update failed: the license has been installed before.

The temporary license file cannot be replaced by a permanent one.

Update failed: the period license cannot replace permanent license.

The specified license file is not on the device before the corresponding feature of the license file is to be installed first.

Update failed: now the system does not have the license.

Try "license install" instead.

The license file is updated successfully and the evaluation license file becomes permanent (use the license file for VSD as an example).

Update success, temporary license LIC-VSD changes into permanent.

- Common** Install a license file that does not belong to the present device.
- Errors**
 - Replace the license file of the new version with the old version.
 - Reinstall an updated license file.
 - Replace the permanent license file with the temporary license file.
 - Start update when the corresponding feature is not licensed for the system.

11.7 show license

Use this command to check a license file for the device.

show license { **all-license** | **dev-license** | **file** [*license*] }

Parameter Description	Parameter	Description
	all-license	The list of all license files already installed on the device
	dev-license	The list of the license files on all devices
	file <i>filename</i>	The name of a specified license file

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization. It displays the license information of the system.

Configuration Examples The following example displays the information of a license file for VSD.

```
Ruijie#show license file LIC-VSD
Service name: LIC-VSD
Attribute: Temporary, Single instance, Releasable
Left days: 362
```

```
Licensed serial number: LIC-VSD00000012268888
```

The following example displays the information of all the license files installed in the system.

```
Ruijie#show license all-license
Searching license in the system...
1. Service name: LIC-AP-64
   Attribute: Releasable
   [Permanent licenses]      [Licensed serial number]
19880966.lic                 LIC-AP-6400000012264966
19880988.lic                 LIC-AP-6400000012264988

   [Temporary license]      [Licensed serial number]
19880900.lic                 LIC-AP-6400000012264900
   (63 days left)

2. Service name: LIC-VSD
   Attribute: Temporary, Releasable
   Left days: 362
   Licensed serial number: LIC-VSD00000012268888
```

The following example displays the information of the license files on all devices.

```
Ruijie#show license dev-license
Searching license in the system...
Dev:1
1. Service name: LIC-AP-64
   Attribute: Releasable
   [Permanent licenses]      [Licensed serial number]
19880966.lic                 LIC-AP-6400000012264966
19880988.lic                 LIC-AP-6400000012264988

   [Temporary license]      [Licensed serial number]
19880900.lic                 LIC-AP-6400000012264900
   (63 days left)

2. Service name: LIC-VSD
   Attribute: Temporary, Releasable
   Left days: 362
   Licensed serial number: LIC-VSD00000012268888
Dev:2
1. Service name: LIC-FC-BLADE-S
   Attribute: Temporary, Releasable
   Left days: 99
   Licensed serial number: LIC-FC-BLADE-S 00000001884686
2. Service name: LIC-AP
   Attribute: Permanent, Releasable
   [Installed licenses]      [Licensed serial number]
```

```

19880921.lic          LIC-AP00000012265001
19880922.lic          LIC-AP00000012265002

```

Field Description:

Field	Description
Service name	The name of the feature of the license file
Attribute	Some features of the license file
Left days	The remaining days of the expiry time of the license file
Installed license	Installed license file
Licensed serial number	License code

11.8 show license hostid

Use this command to display the host ID for the license (one device).

show license hostid

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization. There is a unique serial number for identifying each device.

Configuration Examples The following example displays the host ID for the license (one device).

```

Ruijie#show license hostid
1234942570021

```

11.9 show license unbind-code

Use this command to display the unbound license code on the current device.

show license unbind-code

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require license.

Configuration Examples The following example displays unbound license code on the current device.

```
Ruijie#show license unbind-code
LICENSE                UNBINDING-CODE
LIC-VSD00000012264933
77571FF68737BFF69FF55FF557F55FF57575B595E58587857FF59FF59765AFF55FF5
LIC-FCOE00000012264966
77571FF68737BFF69FF55FF557F55FF57575B595E5B5B7857FF59FF59765AFF55FF5
LIC-TRILL00000012264988
77571FF68737BFF69FF55FF557F55FF57575B595E5D5D7857FF59FF59765AFF5
5FF5
```

Field	Description
LICENSE	Unbound license code.
UNBINDING-CODE	Authenticode for license unbinding.

11.10 show license usage

Use this command to display the status of current license file in the system.

show license usage

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization.

Configuration Examples The following example displays the status of current license file in the system.

```
Ruijie#show license usage
Searching license in the system...
1. Service name: LIC-AP-64
```

```

Attribute: Releasable
[Permanent licenses]      [Licensed serial number]
19880966.lic              LIC-AP-6400000012264966
19880988.lic              LIC-AP-6400000012264988

[Temporary license]      [Licensed serial number]
19880900.lic              LIC-AP-6400000012264900
(63 days left)

2. Service name: LIC-VSD
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888
    
```

Field Description

Field	Description
Service name	The feature name of the license file
Attribute	The attributes of the license file
Left days	The remaining days of the expiry time of the license file

12 Module Hot-plugging Commands

12.1 remove configuration module slot-num

Use this command to remove the module configurations.

remove configuration module *slot-num*

Parameter Description	Parameter	Description
	<i>slot-num</i>	Slot number.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide Use this command to remove the module configurations. This command is invalid for module in on-line status. If there is a module inserted in the slot, this module will be reset.

Configuration

Examples Ruijie(config)# remove configure module 4

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.2 remove configure device device-id

Use this command to remove the configuration on a VSU device, which validates in VSU mode after restart.

remove configure device *device-id*

Parameter Description	Parameter	Description
	<i>device-id</i>	The chassis number.

Defaults N/A

Command Global configuration mode

Mode

Usage Guide This command is used to remove the configuration on a VSU device. It validates after the device is restarted.

Configuration The following example clears the configuration on device 1.

Examples

```
Ruijie(config)# remove configure device 1
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

12.3 reset module slot-num

Use this command to reset a module.

reset module *slot-num*

**Parameter
Description**

Parameter	Description
<i>slot-num</i>	Slot number.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide Use this command to reset a module.

Configuration

Examples

```
Ruijie# reset module 4
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

12.4 show alarm

Use this command to display system alarm messages, concerning card startup failure, temperature, power, and fan alarms.

show alarm

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays system alarm messages.

```
Ruijie#show alarm
Dev  Module          Level  Info
---  -
1    DEV              Warning Some fans are absent.
1    DEV              Critical Some cards are in cannot-startup state.
```

Field	Description
Dev	Device ID
Module	Service module
Level	Alarm level, including Critical and Warning
Info	Alarm cause, such as system power shortage fan absence and card startup failure

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.5 show manuinfo

Use this command to display asset information about all independent components in the system for asset management, including the chassis, fan, power, management board, and line card. The

information covers the ID, slot number, name, serial number (SN), software and hardware version, and MAC address. Not all devices support display of the same information and only supported information is printed.

show manuinfo

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display asset information about all independent components in the system

Configuration The following example displays asset information of the single physical device.

Examples

```
Ruijie#show manuinfo
Device 1
  Location:                Chassis
  Device name:             RG S12006
  Device Serial Number:    62150129A8B0DAF0F0321
  Hardware Version:        V1.0
  Mac Address:             00.D0.F8.00.11.22

Device 2
  Location:                Slot-M1
  Device name:             M12000 CM
  Device Serial Number:    32150129A8B0DAF0F0321
  Hardware Version:        V1.0
  Software Version:        RGOS 10.4(3b17) Release 129646
  Mac Address:             00.D0.F8.00.11.34

Device 3
  Location:                Slot-1
  Device name:             M12000-04XFP-EA
  Device Serial Number:    32150129A8B0DAF0F0322
  Hardware Version:        V1.0
  Software Version:        RGOS 10.4(3b17) Release 129646

Device 4
  Location:                Slot-2
  Device name:             M12000-04XFP-EA
  Device Serial Number:    32150129A8B0DAF0F0323
```

```
Hardware Version:      V1.0
Software Version:      RGOS 10.4(3b17) Release 129646
```

Device 5

```
Location:              Power 1
Device name:           RG PD1200I
Device Serial Number:  42150129A8B0DAF0F0321
Hardware Version:      V1.0
```

Device 6

```
Location:              Power 2
Device name:           RG PD1200I
Device Serial Number:  42150129A8B0DAF0F0322
Hardware Version:      V1.0
```

Device 7

```
Location:              FAN
Device name:           M12000 FAN
Device Serial Number:  52150129A8B0DAF0F0321
Hardware Version:      V1.0
```

The following example displays asset information in VSU mode.

```
Ruijie#show manuinfo
```

Device 1

```
Location:              Chassis 1
Device name:           RG S12006
Device Serial Number:  62150129A8B0DAF0F0321
Hardware Version:      V1.0
Mac Address:           00.D0.F8.00.11.22
```

Device 2

```
Location:              Slot-1/M1
Device name:           M12000 CM
Device Serial Number:  32150129A8B0DAF0F0321
Hardware Version:      V1.0
Software Version:      RGOS 10.4(3b17) Release 129646
Mac Address:           00.D0.F8.00.11.56
```

Device 3

```
Location:              Slot-1/1
Device name:           M12000-04XFP-EA
Device Serial Number:  32150129A8B0DAF0F0322
Hardware Version:      V1.0
Software Version:      RGOS 10.4(3b17) Release 129646
```

```
Device 4
  Location:                Slot-1/2
  Device name:             M12000-04XFP-EA
  Device Serial Number:    32150129A8B0DAF0F0323
  Hardware Version:        V1.0
  Software Version:        RGOS 10.4(3b17) Release 129646

Device 5
  Location:                Power 1/1
  Device name:             RG PD1200I
  Device Serial Number:    42150129A8B0DAF0F0321
  Hardware Version:        V1.0

Device 6
  Location:                Power 1/2
  Device name:             RG PD1200I
  Device Serial Number:    42150129A8B0DAF0F0322
  Hardware Version:        V1.0

Device 7
  Location:                FAN 1
  Device name:             M12000 FAN
  Device Serial Number:    52150129A8B0DAF0F0322
  Hardware Version:        V1.0

Device 8
  Location:                Chassis 2
  Device name:             RG S12006
  Device Serial Number:    62150129A8B0DAF0F0322
  Hardware Version:        V1.0
  Software Version:        RGOS 10.4(3b17) Release 129646
  Mac Address:             00.D0.F8.00.11.33

Device 9
  Location:                Slot-2/M1
  Device name:             M12000 CM
  Device Serial Number:    32150129A8B0DAF0F0324
  Hardware Version:        V1.0
  Software Version:        RGOS 10.4(3b17) Release 129646
  Mac Address:             00.D0.F8.00.11.22

Device 10
  Location:                Slot-2/1
  Device name:             M12000-04XFP-EA
```



```

Device Serial Number:      32150129A8B0DAF0F0325
Hardware Version:         V1.0
Software Version:         RGOS 10.4(3b17) Release 129646

Device 11
Location:                 Slot-2/2
Device name:              M12000-04XFP-EA
Device Serial Number:     32150129A8B0DAF0F0326
Hardware Version:         V1.0
Software Version:         RGOS 10.4(3b17) Release 129646

Device 12
Location:                 Power 2/1
Device name:              RG PD1200I
Device Serial Number:     42150129A8B0DAF0F0323
Hardware Version:         V1.0

Device 13
Location:                 Power 2/2
Device name:              RG PD1200I
Device Serial Number:     42150129A8B0DAF0F0324
Hardware Version:         V1.0

Device 14
Location:                 FAN 2
Device name:              M12000 FAN
Device Serial Number:     52150129A8B0DAF0F0322
Hardware Version:         V1.0

```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

12.6 show sysmac

Use this command to display the MAC address of the current system.

show sysmac

**Parameter
Description**

Parameter	Description
-----------	-------------

N/A	N/A
-----	-----

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays the MAC address of the current system.

Examples

```
Ruijie#show sysmac
00d0.f822.33e2
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

12.7 show version module detail [*module-num*]

Use this command to display the details of the module.

show version module detail [*module-num*]

Parameter Description	Parameter	Description
	<i>module-num</i>	(Optional) Module number.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display details of the module

Configuration Ruijie# **show version module detail 2**

Examples

```
Device : 1
Slot   : 2
User Status : none
Software Status: none
Online Module :
Type   :
Ports  : 0
```

```

Version :
Configured Module :
Type :
Ports :
Version :
Ruijie#
    
```

Related Commands	Command	Description
		show version slots

Platform N/A
Description

12.8 show version slots [slot-num]

Use this command to display the details of the slot.

show version slots [*slot-num*]

Parameter Description	Parameter	Description
		<i>num</i>

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

```

Configuration Examples
Ruijie# show version slots
Dev Slot  Configured Module  Online Module  User Status  Software Status
-----
1 1      none              none
1 2  M8606-24SFP/12GT  M8606-24SFP/12GT  installed  none
1 3  M8606-2XFP       M8606-2XFP       uninstalled  cannot startup
1 4  M8606-24GT/12SFP M8606-24GT/12SFP  installed  ok
1 M1  M8606-CM        M8606-CM                master
1  M2
    
```

Related Commands	Command	Description
		show version moduel detail

Platform N/A
Description

12.9 sysmac

Use this command to configure a MAC address for the system. Use the **no** form of this command to remove the setting.

sysmac
no sysmac

Parameter Description	Parameter	Description
	<i>mac-address</i>	Configures a MAC address for the system.

Defaults N/A

Command Mode Global configuration mode

- Usage Guide**
1. In general, the MAC address is programmed on the management board or the chassis flash. In virtual switching unit (VSU) mode, the system saves the MAC address in use in the configuration file to avoid flow interruption caused by MAC address change. The valid MAC address saved in the configuration file validates in preference after the device is restarted.
 2. The MAC address of the gateway may be bound on some downstream devices. If the system is configured with the **auth-mode gateway** command, you can use the **sysmac** command to replace the MAC address of the gateway without changing the MAC address configuration on the downstream devices.
 3. The configuration takes effect after the device is restarted.

Configuration Examples The following example deletes the MAC address saved in the configuration file.

```
Ruijie#no sysmac
```

The following example configures MAC address 00d0.f822.33e2 for the system.

```
Ruijie#sysmac 00d0.f822.33e2
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

13 Supervisor Module Redundancy Commands

13.1 auto-sync time-period

Use this command to configure the auto-sync time-period of running-config and startup-config when the dual supervisor module is redundant. Use the **no** form of this command to disable automatic synchronization for the dual supervisor modules. Use the **default** form of this command to restore the default automatic synchronization time period for the dual supervisor modules.

auto-sync time-period *value*

no auto-sync time-period

default auto-sync time-period

Parameter Description	Parameter	Description
	<i>value</i>	Automatic synchronization time interval measured in seconds, in the range from one second to one month (2,678,400 seconds).

Defaults The default is one hour (3600 seconds) by default.

Command Mode Redundancy configuration mode

Usage Guide N/A

Configuration Examples The following example sets the automatic synchronization interval to 60 seconds.

```
Ruijie(config)# redundancy
Ruijie(config-red)# auto-sync time-period 60
Redundancy auto-sync time-period: enabled (60 seconds).
Ruijie(config-red)# exit
```

The following example disables automatic synchronization.

```
Ruijie(config)# redundancy
Ruijie(config-red)# no auto-sync time-period
Redundancy auto-sync time-period: disabled.
Ruijie(config-red)# exit
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.2 redundancy

Use this command to enter redundancy configuration mode.

redundancy

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example enters redundancy configuration mode.

Examples

```
Ruijie# config terminal
Ruijie(config)# redundancy
Ruijie(config-red)# exit
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.3 redundancy forceswitch

Use this command to perform active/standby supervisor module switchover.

redundancy forceswitch

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

- Usage Guide** If this command is executed on the active supervisor module, the module will be reset and the standby supervisor module will act as an active supervisor module.
- The following conditions are required to perform hot backup switchover:
- This command is executed on the active supervisor module. There is a standby supervisor module.

Configuration The following example performs active/standby supervisor module switchover.

Examples

```
Ruijie# redundancy forceswitch
This operation will reload the master unit and force switchover to the slave
unit. Are you sure to continue? [N/y] y
```

**Related
Commands**

Command	Description
reload	Resets the active supervisor module.

Platform N/A


Description

13.4 redundancy reload

Use this command to reset the supervisor module.

redundancy reload { peer | shelf [switchid] }

**Parameter
Description**

Parameter	Description
peer	Resets the standby supervisor module.
shelf	Resets both the active and standby supervisor modules on the device which works as a single physical device. The device ID should be specified on the device which works as a Virtual Switching Unit (VSU) device.
<i>switchid</i>	VSU device ID, supported on a VSU device.  This parameter is not supported in stand-alone mode. It must be contained in the redundancy reload shelf command in VSU mode.

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide Resetting the supervisor module does not affect data forwarding. Data forwarding will not be interrupted and the user session information will not be missing.

The **redundancy reload shelf** command is used to reset the device which works as a single physical device. The **redundancy reload shelf *switchid*** command is used to reset the specified device which works as a VSU device.

Configuration The following example resets the standby supervisor module.

Examples

```
Ruijie# redundancy reload peer
This operation will reload the current slave unit. Are you sure to continue?
[N/y] y
Preparing to reload peer!
```

The following example resets device 2 which works as a VSU device.

```
Ruijie# redundancy reload shelf 2
This operation will reload the device 2. Are you sure to continue? [N/y] y
Preparing to reload device 2!
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

13.5 show redundancy states

Use this command to display the current redundancy state.

show redundancy states

Parameter Description

Parameter	Description
states	Displays the redundancy status of the active or the standby devices.

Defaults N/A

Command Mode User EXEC mode / Privileged EXEC mode

Usage Guide Currently, only 1:1 hot backup (for the global active module and standby module) is supported in the VSU mode. Therefore, only the hot backup state of the local and peer device is displayed.

Configuration The following example displays the redundancy states of active supervisor module.

Examples

```
Ruijie> enable
Ruijie# show redundancy states
Redundancy role: master
```



```
Redundancy state: realtime
Auto-sync time-period: 3600 s
```

The following example displays the redundancy state of the standby supervisor module.

```
Ruijie> enable
Ruijie# show redundancy states
Redundancy role: slave
Redundancy state: realtime
```

The following example displays the redundancy state of the candidate supervisor module.

```
Ruijie> enable
Ruijie# show redundancy states
Redundancy role: candidate
Redundancy state: none
```

Field	Description
role	The role of the supervisor module.
state	The state of the supervisor module.
Auto-sync time-period	Displayed on the active supervisor module. The configuration file synchronizes the time interval automatically. "disabled" indicates no automatic synchronization.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14 USB Commands

14.1 show usb

Use this command to display the information about the inserted USB device in the system.

show usb

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Device information is displayed if there is a USB device. Otherwise, there is no output. If the USB disk is connected to the USB port on the device, the ID displayed by running the show usb command is X, the USB port number. If the USB disk is connected to the USB port on the device via a HUB, the ID displayed by running the show usb command is X-Y, in which X stands for the USB port number and Y for the HUB slot number.

Configuration The following example displays the information about the USB device:

Examples

```
Ruijie# show usb
Device: Mass Storage:
ID: 0
URL prefix: usb0
Disk Partitions:
usb0 (type:FAT32)
Size : 131,072,000B(125MB)
Available size: 1,260,020B(1.2MB)
```

In above information, the Mass Storage Device is the name of the device.

The meaning of the information is as below:

Table 1: the description of the field.

Field	Description
URL	Prefix used to access the USB device.
Size	Accessible size of the USB device.
Available size	Available size of the USB device.

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

14.2 usb remove

Use this command to remove the USB device.

usb remove *device_id*

Parameter Description	Parameter	Description
	device_id	Device ID of USB to be removed.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Before pulling out the USB device, you need to remove the device using a command, so as to prevent errors that may occur because the system is using the device. If the device is removed successfully, the system will show a prompt, when you can pull out the device. If the device cannot be pulled out, it indicates that the system is using this USB device, so you have to wait a moment before removing it again.

Configuration Examples The following example removes the USB device.

```
Ruijie# usb remove 0
OK, now you can pull out the device 0.
*Jan 1 00:18:16: %USB-5-USB_DISK_REMOVED: USB Disk <Mass Storage> has been
removed from USB port 0!
```

At this moment, the USB device can be plugged out.

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

15 PoE Management Commands

15.1 poe alloc-power

Use this command to set the allocation power for the port. Use the **no** or **default** form of this command to restore the default allocation power.

poe alloc-power *int*

no poe alloc-power

default poe alloc-power

Parameter	Parameter	Description
Description	<i>int</i>	The maximum power, in the range from 0 to 30W.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the allocation power for port GigabitEthernet 0/1 to 20W.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe alloc-power 20
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

15.2 poe class-lldp enable

Use this command to configure LLDP two-event classification. Use the **no** or **default** form of this command to restore the default setting.

poe class-lldp enable

no poe class-lldp enable

default poe class-lldp enable

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example enables LLDP two-event classification.

Examples

```
Ruijie(config)# poe class-lldp enable
Ruijie(config)# end
Ruijie#write
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

15.3 poe enable

Use this command to enable the power over Ethernet (PoE) function on the interface. Use the **no** form of this command to disable this function.

poe enable
no poe enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default,

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example disables the PoE function on port GigabitEthernet 0/1,

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no poe enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

15.4 poe enable pse [device device_num] slot slot_num

Use this command to enable PoE for the line card. Use the **no** or **default** form of this command to disable this function.

poe enable pse [device device_num] slot slot_num

no poe enable pse [device device_num] slot slot_num

default poe enable pse [device device_num] slot slot_num

Parameter Description	Parameter	Description
		<i>device_num</i>
	<i>slot_num</i>	The slot number.

Defaults This function is enabled by default.

Command Global configuration mode

Mode

Usage Guide N/A

Configuration The following example disables PoE for line card 2.

Examples

```
Ruijie# configure
Ruijie(config)# no poe enable pse slot 2
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

15.5 poe legacy

Use this command to enable non-standard PD compatibility. Use the **no** or **default** form of this command to restore the default setting.

poe legacy

no poe legacy

default poe legacy

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example enables non-standard compatibility for port GigabitEthernet 0/1.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe legacy
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

15.6 poe max-power

Use this command to set the maximum power for the port. Use the **no** or **default** form of this command to restore the default setting,

poe max-power *int*

no poe max-power

default poe max-power

Parameter Description	Parameter	Description
	<i>int</i>	The maximum power, in the range from 0 to 30W. Note that this parameter is in the range from 0 to 15.4W on the system supporting 802.3af only. HPoE port ID is in the range from 0

	to 90.
--	--------

Defaults The maximum power is not set by default.

Command Interface configuration mode

Mode

Usage Guide N/A.

Configuration The following example sets the maximum power for port GigabitEthernet 0/1 to 20W.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe max-power 20
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

15.7 poe max-power max-power pse [device device_num] slot slot_num

Use this command to set the maximum PoE power for the line card. Use the **no** or **default** form of this command to restore the default setting.

poe max-power *max-power* **pse** [**device** *device_num*] **slot** *slot_num*

no poe max-power *max-power* **pse** [**device** *device_num*] **slot** *slot_num*

default poe max-power *max-power* **pse** [**device** *device_num*] **slot** *slot_num*

**Parameter
Description**

Parameter	Description
<i>max-power</i>	The maximum power, in the range from 0 to 1440W.
<i>device_num</i>	In stand-alone mode, keyword device is not displayed; in VSU mode, this parameter indicates the corresponding chassis or device. If keyword device is displayed, this parameter indicates the master chassis or device.
<i>slot_num</i>	The slot number

Defaults The default *max-power* is 369.6W for the 24-port line card and 739.2W for the 48-port line card.

Command Global configuration mode

Mode

Usage Guide N/A

Configuration The following example sets the maximum PoE power for line card 2 to 300W.

Examples

```
Ruijie(config)# poe max-power 300 pse slot 2
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

15.8 poe mode

Use this command to set the PoE management mode. Use the **no** or **default** form of this command to restore the default setting.

poe mode { auto | energy-saving | static }

no poe mode

default poe mode

**Parameter
Description**

Parameter	Description
auto	Sets the power management mode to auto mode, the default mode.
energy-saving	Sets the power management mode to energy-saving mode, the optional mode,
static	Sets the power management mode to static mode, the optional mode,

Defaults The default mode is auto.

**Command
Mode** Global configuration mode

Usage Guide N/A

Configuration The following example sets the PoE management mode to energy-saving mode.

Examples

```
Ruijie# configure
Ruijie(config)# poe mode energy-saving
Ruijie(config)# end
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

15.9 poe notification-control enable

Use this command to enable Trap notification in PoE MIB(RFC3621). Use the **no** or **default** form of this command to restore the default setting.

poe notification-control enable

no poe notification-control enable

default poe notification-control enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables Trap notification in PoE MIB(RFC3621).

```
Ruijie(config)# poe notification-control enable
Ruijie(config)# end
Ruijie#write
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

15.10 poe pd-description

Use this command to set the PD descriptor for the port. Use the **no** or **default** form of this command to restore the default setting.

poe pd-description *pd-name*

no poe pd-description

default poe pd-description

Parameter Description	Parameter	Description
	<i>pd-name</i>	PD descriptor name, a string no more than 32 characters.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the PD descriptor for port GigabitEthernet 0/1.

Examples

```
Ruijie# configure
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe pd-description ap220
Ruijie(config-if-GigabitEthernet 0/1)# end
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

15.11 poe power-off time-range name

Use this command to configure scheduled power-on for the port. Use the **no** or **default** form of this command to restore the default setting.

poe power-off time-range *name*

no poe power-off time-range

default poe power-off time-range

Parameter Description

Parameter	Description
<i>name</i>	Time-range name.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the port GigabitEthernet 0/1 to be disabled from 8:30 to 17:30 every day.

Examples

```
Ruijie# configure
Ruijie(config)# time-range poe-time
Ruijie(config-time-range)# periodic weekdays 8:30 to 17:30
Ruijie(config-time-range)# exit
```

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe power-off time-range poe-time
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A**Description**

15.12 poe priority

Use this command to set the PoE priority for the port. Use the **no** or **default** form of this command to restore the default setting.

poe priority { low | high | critical }

no poe priority

default poe priority

**Parameter
Description**

Parameter	Description
{ low high critical }	Priority level.

Defaults The default is low.**Command
Mode** Interface configuration mode**Usage Guide** N/A**Configuration** The following example sets the PoE priority for port GigabitEthernet 0/1 to critical.**Examples**

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe priority critical
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A**Description**

15.13 poe priority { critical | high | low } pse [device device_num] slot slot_num

Use this command to set the PoE priority for the line card. Use the **no** or **default** form of this command to restore the default setting,

poe priority { low | high | critical } pse [device device_num] slot slot_num

no poe priority { low | high | critical } pse [device device_num] slot slot_num

default poe priority { low | high | critical } pse [device device_num] slot slot_num

Parameter Description	Parameter	Description
	{ low high critical }	Priority level.
	device_num	In stand-alone mode, keyword device is not displayed; in VSU mode, this parameter indicates the corresponding chassis or device. If keyword device is displayed, this parameter indicates the master chassis or device.
	slot_num	The slot number.

Defaults The default is low.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the PoE priority for line card 2 to high.

```
Ruijie(config)# poe priority high pse slot 2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

15.14 poe reserve-power

Use this command to set the reserve power for the system in energy-saving mode. Use the **no** or **default** form of this command to restore the default setting,

poe reserve-power int

no poe reserve-power

default poe reserve-power

Parameter Description	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>int</i></td> <td>Reserve power percentage, in the range from 0 to 50.</td> </tr> </tbody> </table>	Parameter	Description	<i>int</i>	Reserve power percentage, in the range from 0 to 50.
Parameter	Description				
<i>int</i>	Reserve power percentage, in the range from 0 to 50.				
Defaults	N/A				
Command Mode	Global configuration mode				
Usage Guide	N/A				
Configuration Examples	<p>The following example sets the reserve power for the system to 10%.</p> <pre>Ruijie(config)# poe reserve-power 10 Ruijie(config)# end</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

15.15 poe uninterruptible-power

Use this command to configure uninterruptible warm start, Use the **no** or **default** form of this command to restore the default setting.

poe uninterruptible-power

no poe uninterruptible-power

default no poe uninterruptible-power

Parameter Description	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
Defaults	This function is disabled by default.				
Command Mode	Global configuration mode				
Usage Guide	This function takes effect when the device is started after the configuration is saved.				
Configuration Examples	<p>The following example enables uninterruptible PoE for warm start and saves configuration.</p> <pre>Ruijie(config)# poe uninterruptible-power</pre>				

```
Ruijie(config)# end
Ruijie#write
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

15.16 poe warning-power

Use this command to set the power alarm threshold for the system. Use the **no** or **default** form of this command to restore the default setting,

```
poe warning-power int
no poe warning-power
default poe warning-power
```

Parameter Description

Parameter	Description
<i>int</i>	Power alarm threshold (percentage), in the range from 0 to 99.

Defaults The default is 99.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the power alarm threshold for the system to 80%.

```
Ruijie(config)# poe warning-power 80
Ruijie(config)# end
Ruijie#write
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

15.17 show poe interface

Use this command to display PoE configuration and status of the specified port.

show poe interface *interface-name*

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the PoE configuration and status in interface GigabitEthernet 0/1.

Examples Ruijie#show poe interface GigabitEthernet 0/1

```

Interface           : Gi0/1
Power enabled       : enable
Power status        : on
Max power           : N/A
Allocate power      : N/A
Current power       : 14.8 W
Average power       : 14.8 W
Peak power          : 14.8 W
Voltage             : 53.5 V
Current             : 278 mA
PD class            : 4
Trouble cause       : None
Priority             : critical
Legacy              : off
Power-off time-range : N/A
Power management    : auto
4pair status        : normal

```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

15.18 show poe interfaces

Use this command to display PoE status or configuration of all ports.

show poe interfaces status

show poe interfaces configuration

Parameter Description	Parameter	Description
	status	Displays PoE status of all ports.
	configuration	Displays PoE configuration of all ports.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide This command is used to display PoE status or configuration of all ports.

Configuration The following example displays PoE status of all ports.

Examples

```
Ruijie#show poe interfaces status
Interface Power   Power   Curr  Avg   Peak  Curr   Trouble PD   Port
          Control Status Power Power Power Current Cause  Class Voltage
-----
Gi0/1    enable on    14.8W 14.8W 14.8W 278mA  0     4    53.5V
Gi0/2    enable on    28.4W 28.4W 28.4W 531mA  0     4    53.5V
Gi0/3    enable on    14.9W 14.9W 14.9W 279mA  0     4    53.5V
Gi0/4    enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/5    enable on    14.8W 14.8W 14.8W 278mA  0     4    53.5V
Gi0/6    enable on    15.0W 15.0W 15.0W 281mA  0     4    53.5V
Gi0/7    enable on    6.1W  6.1W  6.1W  115mA  0     4    53.5V
Gi0/8    enable on    14.8W 14.8W 14.8W 277mA  0     4    53.5V
Gi0/9    enable on    14.7W 14.7W 14.7W 276mA  0     4    53.5V
Gi0/10   enable on    14.8W 14.8W 14.8W 278mA  0     4    53.5V
Gi0/11   enable on    14.7W 14.7W 14.7W 275mA  0     4    53.5V
Gi0/12   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/13   enable on    14.8W 14.8W 14.8W 278mA  0     4    53.5V
Gi0/14   enable on    0.3W  0.3W  0.3W  7mA    0     4    53.5V
Gi0/15   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/16   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/17   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/18   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/19   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/20   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
Gi0/21   enable off    0.0W  0.0W  0.0W  0mA    6     N/A  0.0V
```

```

Gi0/22  enable off    0.0W 0.0W 0.0W 0mA   6   N/A  0.0V
Gi0/23  enable off    0.0W 0.0W 0.0W 0mA   6   N/A  0.0V
Gi0/24  enable off    0.0W 0.0W 0.0W 0mA   6   N/A
0.0V

```

The following example displays PoE configuration of all ports.

```

Ruijie#show poe interfaces configuration
Interface Power      Power  Max   Alloc Port      Port  Power-off
          Control  Status Power Power Power Priority Legacy Time-range
-----
Gi0/1    enable  on    N/A   N/A   critical off    N/A
Gi0/2    enable  on    N/A   N/A   critical off    N/A
Gi0/3    enable  on    N/A   N/A   critical off    N/A
Gi0/4    enable  off   N/A   N/A   critical off    N/A
Gi0/5    enable  on    N/A   N/A   critical off    N/A
Gi0/6    enable  on    N/A   N/A   high    off    N/A
Gi0/7    enable  on    N/A   N/A   high    off    N/A
Gi0/8    enable  on    N/A   N/A   high    off    N/A
Gi0/9    enable  on    N/A   N/A   high    off    N/A
Gi0/10   enable  on    N/A   N/A   high    off    N/A
Gi0/11   enable  on    N/A   N/A   high    off    N/A
Gi0/12   enable  off   N/A   N/A   high    off    N/A
Gi0/13   enable  on    N/A   N/A   low     off    N/A
Gi0/14   enable  on    N/A   N/A   low     off    N/A
Gi0/15   enable  off   N/A   N/A   low     off    N/A
Gi0/16   enable  off   N/A   N/A   low     off    N/A
Gi0/17   enable  off   N/A   N/A   low     off    N/A
Gi0/18   enable  off   N/A   N/A   low     off    N/A
Gi0/19   enable  off   N/A   N/A   low     off    N/A
Gi0/20   enable  off   N/A   N/A   low     off    N/A
Gi0/21   enable  off   N/A   N/A   low     off    N/A
Gi0/22   enable  off   N/A   N/A   low     off    N/A
Gi0/23   enable  off   N/A   N/A   low     off    N/A
Gi0/24   enable  off   N/A   N/A   low     off    N/A

```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

15.19 show poe powersupply

Use this command to display the PoE power supply status.

show poe powersupply

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the PoE power supply status.

```

Ruijie#show poe powersupply
Device member          : 1
Power management      : auto
PSE total power       : 1000W
PSE total power consumption : 300W
PSE total remain power : 700W
PSE total powered port : 0
PSE disconnect mode   : dc
PSE reserve power     : 0%
PSE warning power     : 99%
PSE class lldp        : disable
PSE uninterruptible-power : disable
  PSE member          : 1
    PSE Power status : normal      PSE Power
Enabled              : enable
  PSE max power      : 300W
  PSE priority       : low
  PSE alloc power    : 300W
  PSE available power : 300W
  PSE total power consumption : 0 W
  PSE total remain power : 300W
  PSE peak power     : 0 W
  PSE average power  : 0 W
  PSE powered port   : 0

```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

16 UFT Commands

16.1 show switch-mode status

Use this command to display the UFT mode of a switch.

show switch-mode status

Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example displays the UFT mode of the switch in stand-alone mode.	
	<pre>Ruijie(config)#show switch-mode status Slot No Switch-Mode 3 bridge</pre>	
	2The following example displays the UFT mode of the switch in VSU mode.	
	<pre>Ruijie(config)#show switch-mode status Slot No Switch-Mode switch 1 slot 3 bridge</pre>	
	Field Description:	
	Field	Description
	<i>Slot No</i>	Displays only slot No. in stand-alone mode; displays both device No. and slot No. in VSU mode.
	<i>Switch-Mode</i>	Indicates the UFT operating mode.
Prompt Messages	N/A	
Platforms	N/A	

16.2 switch-mode mode_type slot slot_num

Use this command to switch the UFT operating mode for a line card in stand-alone mode.

switch-mode *mode_type* **slot** *slot_num*

Use this command to restore the Default UFT operating mode for the specified line card in stand-alone mode.

no switch-mode *mode_type* **slot** *slot_num*

Parameter Description	Parameter	Description
	<i>mode_type</i>	<p>Indicates the UFT operating mode.</p> <p>In stand-alone mode, the line card can operate in the following modes:</p> <p>Default: Default mode, which is applied to most of application scenarios.</p> <p>bridge: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate.</p> <p>gateway: Gateway mode, which is applied to the application scenario in which Layer 3 services dominate.</p> <p>gateway-max: Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed.</p> <p>gateway-ndmax: Gateway-ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed.</p> <p>label: Label mode, which is applied to the application scenarios that require a great amount of MPLS labels.</p> <p>route-v4max: IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes.</p> <p>route-v6max: IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.</p> <p>acl: acl mode, which is applied to the application scenarios that require ACL and other security functions.</p> <p>acl-ipv4: acl-ipv4 mode, which is applied to the application scenarios that require many ACLs and some IPv6 routes.</p> <p>mc: multicast mode, which is applied to the application scenarios that require a great number of multicast routes.</p>
	<i>slot_num</i>	Indicates the corresponding line card installed in the chassis.

Defaults The Default UFT operating mode is Default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example switches the UFT operating mode of the line card in slot 3 of the switch to bridge mode in stand-alone mode.

```
Ruijie(config)#switch-mode bridge slot 3
Please save current config and restart your device!
Ruijie(config)#show run

Building configuration...
Current configuration : 1366 bytes

version 11.0(1B2)
!
cwmmp
!
install 3 M8600E-24XS4QXS-DB
!
sysmac 1414.4b34.5624
!
nfpp
!
switch-mode bridge slot 3
```

Verification Use the show switch-mode status command to display the current operating mode.

```
Ruijie(config)#show switch-mode status
Slot No          Switch-Mode
3                bridge
```

Prompt Messages N/A

Common Errors N/A

Platforms N/A

16.3 switch-mode mode_type switch switch_num slot slot_num

Use this command to switch the UFT mode for a line card in VSU mode.

switch-mode mode_type switch switch_num slot slot_num

Use this command to delete the UFT mode for the specified line card in VSU mode.

no switch-mode mode_type switch switch_num slot slot_num

Parameter Description	Parameter	Description
	<i>mode_type</i>	<p>Indicates the UFT operating mode.</p> <p>In VSU mode, the line card can operate in the following modes:</p> <p>Default: Default mode, which is applied to most of application scenarios.</p> <p>bridge: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate.</p> <p>gateway: Gateway mode, which is applied to the application scenarios in which Layer 3 services dominate.</p> <p>gateway-max: Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed.</p> <p>gateway-ndmax: Gateway_ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed.</p> <p>label: Label mode, which is applied to the application scenarios that require a great amount of MPLS labels.</p> <p>route-v4max: IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes.</p> <p>route-v6max: IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.</p> <p>acl: acl mode, which is applied to the application scenarios that require ACL and other security functions.</p> <p>acl-ipv4: acl-ipv4 mode, which is applied to the application scenarios that require many ACLs and some IPv6 routes.</p> <p>mc: multicast mode, which is applied to the application scenarios that require a great number of multicast routes.</p>
	<i>switch_num</i>	Indicates the chassis or box device number in VSU mode.
	<i>slot_num</i>	Indicates the line card installed in the chassis device.

Defaults The default UFT operating mode is default configuration.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example switches the UFT operating mode of the line card in slot 3 of switch1 to bridge mode in VSU mode.

```
Ruijie(config)#switch-mode bridge switch 1 slot 3
Please save current config and restart your device!
Ruijie(config)#show run
```



```
Building configuration...
Current configuration : 1485 bytes

version 11.0(1B2)
!
cswmp
!
install switch 1 RG-S7805E
install 1/3 M8600E-24XS4QXS-DB
!
sysmac 1414.4b34.5624
!
nfpp
!
switch-mode bridge switch 1 slot 3
```

Verification Use the show switch-mode status command to display the UFT mode.

```
Ruijie(config)#show switch-mode status
Slot No          Switch-Mode
switch 1 slot 3  bridge
```

Prompt Messages N/A

Common Errors N/A

Platforms N/A

17 PKG_MGMT Commands

17.1 clear storage

Use this command to remove an installation package on the local device.

clear storage [*url*]

Parameter Description	Parameter	Description
	<i>url</i>	A local <i>url</i> directory or full path name indicates where the installation package is stored
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	This command is used to remove an installation package or all packages in a directory and all installation packages on the local device.	
Configuration Examples	<pre>Ruijie#clear storage Remove the whole storage directory?[y/n]y Ruijie#clear storage usb0 Remove the file or directory usb0 from the storage?[y/n]y Ruijie#</pre>	
Verification	Check specified <i>url</i>	
Platforms	N/A	

17.2 patch active

Use this command to activate a patch to take effect.

patch active [*slot* { *num* | **M1** | **M2** | **all** }]

Parameter Description	Parameter	Description
	slot <i>num</i>	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
	slot all	This parameter is used on a chassis device. It indicates all devices.

slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.
slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.

Defaults	N/A
Command Mode	Privileged EXEC mode
Default Level	2
Usage Guide	Activating operation can be performed only on the device already installed with a patch, after which the patch really takes effect. This command can be used to activate a hot patch temporarily. The activated patch becomes invalid after device restart.
Configuration Examples	<p>The following example activates a patch on the box device.</p> <pre>Ruijie#patch active Active the patch package success</pre> <p>The following example activates a patch on the chassis device.</p> <pre>Ruijie#patch active slot 8 [Slot 8]: Active the patch package success</pre>
Verification	Use the show patch command to display patch information.
Prompt Messages	<p>The patch is activated successfully.</p> <pre>Active the patch package success</pre> <p>The running fails and a patch package needs to be installed at first.</p> <pre>Patch not installed</pre> <p>There is no need to run the command for the patch in the activated or running status.</p> <pre>The patch status is already active or running</pre> <p>Contact the service center to solve the package problem.</p> <pre>Cannot find the package's scripts file</pre>
Common Errors	<p>There is no hot patch installed on current device.</p> <p>The hot patch on current device is already activated.</p>

Platforms N/A

17.3 patch deactivate

Use this command to deactivate a patch.

patch deactivate [slot {*num* | **M1** | **M2** | **all** }]

Parameter Description	Parameter	Description
	slot <i>num</i>	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
	slot all	This parameter is used on a chassis device. It indicates all devices.
	slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.
	slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command can be performed to deactivate a patch only after the patch is in the activated status.

Configuration The following example deactivates a patch on the box device.

Examples

```
Ruijie#patch deactivate
Deactivate the patch package success
```

The following example deactivates a patch on the chassis device.

```
Ruijie#patch deactivate slot 8
[Slot 8]:
Deactivate the patch package success
```

Verification Use the **show patch** command to display patch information.

Prompt The patch is deactivated successfully.

Messages

```
Deactivate the patch package success;
```

The running fails and a patch package needs to be installed at first.

```
Patch not installed
```

There is no need to run the command for the patch in the deactivated status.

```
The patch is not in active or running status
```

Contact the service center to solve the package problem.

```
Cannot find the package's scripts file
```

- Common** There is no hot patch installed on current device.
Errors The hot patch on current device is already invalid.

17.4 patch delete

Use this command to uninstall a patch.

```
patch delete[ slot {num | M1 | M2 | all } ]
```

Parameter Description	Parameter	Description
	slot num	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
	slot all	This parameter is used on a chassis device. It indicates all devices.
	slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.
	slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used to remove the existing hot patch package on the device.

Configuration The following example removes the installed hot patch package from the box device.

Examples

```
Ruijie# patch delete
Clear the patch patch_bridge success
Clear the patch success
```

The following example removes the installed hot patch package from the chassis device.

```
Ruijie# patch delete slot M1
[Slot M1]:
Clear the patch patch_bridge success
Clear the patch success
```

Verification Use the **show patch** command to display patch status.

Prompt The patch is uninstalled successfully.

Messages

```
Clear the patch success
```

A hot patch package should be installed at first for it has not been installed.

```
Patch not installed
```

**Common
Errors**

There is no hot patch installed on current device.

17.5 patch running

Use this command to activate a patch permanently.

```
patch running[ slot {num | M1 | M2 | all } ]
```

**Parameter
Description**

Parameter	Description
slot <i>num</i>	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
slot all	This parameter is used on a chassis device. It indicates all devices.
slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.
slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.

**Command
Mode**

Privileged EXEC mode

Default Level

2

Usage Guide

Activating operation can be performed only on the device already installed with a patch, after which the patch really takes effect. This command can be used to activate a hot patch permanently.

**Configuration
Examples**

The following example activates a patch on the box device.

```
Ruijie#patch running
The patch on the system now is in running status
```

The following example activates a patch on the chassis device.

```
Ruijie#patch running slot M1
[Slot M1]:
The patch on the system now is in running status
```

Verification

Use the **show patch** command to display the patch information.

Prompt

The patch is activated permanently.

Messages

The patch on the system now is in running status

The running fails and a patch package needs to be installed at first.

Patch not installed

There is no need to run the command for the patch is in the deactivated status.

The patch is not in active or running status

Contact the service center to solve the package problem.

Cannot find the package's scripts file

Common

There is no hot patch on current device.

Errors

The hot patch is already activated on current device.

17.6 show component

Use this command to display all components already installed on current device and their information.

show component [slot { *num* | M1 | M2 | all }] [*component_name*]

**Parameter
Description**

Parameter	Description
slot <i>num</i>	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
slot all	This parameter is used on a chassis device. It indicates all devices.
slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.
slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.
<i>component_name</i>	Name of the components When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.

Command

Privileged EXEC mode

Mode**Default Level**

2

Usage Guide

This command includes one with *component_name* and one without *component_name*. During

upgrade, it requires users to understand all components installed on current device and their version information before components deletion. This needs to use the **show component** command without *component_name*. The **show component** command with *component_name* is used to obtain details of the corresponding component. The detailed information enables users to easily realize components' operation and damage. It is significant to insure their troubleshooting, security and reliability.

- i Some components in use will change their defaults files. Though this is more possibly normal than malicious, the **show component** command is used only to judge whether component files change in use. It is unable to distinguish natural damage from malicious one. It depends on users to make a further judgment.

Configuration Examples The following example displays all components already installed on the box device and their information.

```
Ruijie# show component
Package :sysmonit
    Version:1.0.1.23cd34aa      Build time: Wed Dec 7 00:58:56 2013
    Size:12877  Install time :Wed Mar 5 14:23:12 2012
    Description: this is a system monit package
    Required packages: None
-----
Package:bridge
    Version:2.0.1.37cd5cda      Build time: Wed Dec 7 00:54:56 2013
    Size:23245  Install time :Wed Mar 5 14:30:12 2012
    Description: this is a bridge package
    Required packages: None
-----
```

This command is used to obtain all components already installed on the device and their basic information. The information offers a basis for users to decide whether to upgrade or delete components.

Field	Description
Package	Name of the component
Version	Version number of the component
Build time	Compilation time of the component on the server
Size	Content size of the component
Install time	Installation time of the component
Description	Simple functional description of the component
Required packages	Name of required packages

The following example displays the information of all feature components already installed on the chassis device.

```
Ruijie#show component slot 8
Ruijie#*
```



```
[Slot 8]:
Package : utils-system
  Version: 1.0.0.433ef8d      Build time: Sun May 19 19:22:54 2013
  Size: 823936   Install time: Sun May 19 19:27:04 2013
  Description: utils system compile
  Required packages: None
-----
Package : tcl-expect
  Version: 1.0.0.433ef8d      Build time: Sun May 19 19:19:18 2013
  Size: 3474153   Install time: Sun May 19 19:27:04 2013
  Description: tcl & expect packages
  Required packages: None
-----
```

The following example displays the information of specified components already installed on the box device.

```
Ruijie# show componentbridge
package:bridge
  Version: 2.3.1.1252ea      Build time: Wed Dec 7 00:54:56 2013
  Size:26945   Install time : Wed Mar 19:23:15 2012
  Description:this is a bridge package
  Required packages: None
  Package files:
    /lib64
    /lib64/libbridge.so
    /sbin
    /sbin/bridge

  Package file validate: [OK]
  Required relationship verify: [OK]
```

The other information except the basic information of components is listed as follows.

Field	Description
Package file validate	Checks whether the component files are intact. "OK" is displayed when all component files work properly; "ERR" is displayed together with their names when some component files are lost or revised.
Required package	Lists all required packages of the component. "OK" is labeled if required components are already installed; "ERR" is labeled if not together with detailed description about their names and versions.
Package files	Lists all files contained in the package.

Prompt The execution is successful with all components information displayed.

Messages

```
Package :sysmonit
  Version:1.0.1.23cd34aa      Build time: Wed Dec 7 00:58:56 2013
  Size:12877 Install time :Wed Mar 5 14:23:12 2012
  Description: this is a system monit package
  Required packages: None
-----
Package:bridge
  Version:2.0.1.37cd5cda      Build time: Wed Dec 7 00:54:56 2013
  Size:23245 Install time :Wed Mar 5 14:30:12 2012
  Description: this is a bridge package
  Required packages: None
-----
```

17.7 show patch

Use this command to display the information of a hot patch package already installed on the device.

show patch [slot {*num* | **M1** | **M2** | **all** }][*patch_name*]

Parameter Description	Parameter	Description
	slot num	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
	slot all	This parameter is used on a chassis device. It indicates all devices.
	slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.
	slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.
	<i>patch_name</i>	Name of the patches When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.

Command Privileged EXEC mode

Mode

Default Level 2

Usage Guide This command is used to check all patches already installed on the device and their information.

Configuration The following example displays all patches already installed on the box device.

Examples

```
Ruijie# show patch
patch package patch_install installed in the system, version:pa1
Package : patch_bridge
status:running
Version: pa1      Build time: Mon May 13 09:03:07 2013
Size: 277      Install time: Tue May 21 03:07:17 2013
      Description: a patch for bridge
      Required packages: None
```

This command is used to obtain the basic information of all patches already installed on the device.

Field	Description
Package	Name of the patch
status	Status of the patch
Version	Version of the patch
Build time	Compilation time of the patch on the server
Size	Content size of the patch
Install time	Installation time of the patch
Description	Simple functional description of the patch

The following example displays the information of all patches installed on the chassis device.

```
Ruijie#show patch slot 8
[Slot 8]:
Patch package patch_install installed in the system, version:pa1
Package : patch_test
Status: running
      Version: 1.0.0.05151504
      Build time: Wed May 15 07:04:28 2013
      Size: 1804
      Install time: Thu Jan 1 00:56:43 1970
      Description: Experimentation
      Required packages: None
-----
```

The following example displays the information of particular patches installed on the box device.

```
Ruijie# show componentbridge
package:bridge
      Version: 2.3.1.1252ea      Build time: Wed Dec 7 00:54:56 2011
      Size:26945 Install time : Wed Mar 19:23:15 2012
      Description:this is a bridge package
      Required packages: None
      Package files:
          /lib64
```

```

/lib64/libbridge.so
/sbin
/sbin/bridge

Package file validate: [OK]

```

The other information except the basic information of the patch is listed as follows:

Field	Description
Package file validate	Checks whether the patch files are intact. "OK" is displayed when all patch files work properly; "ERR" is displayed together with their names when some files are lost or revised.
Package files	Lists all files contained in the patch package.

Prompt

The information of the patch is displayed after successful running.

Messages

```

Patch package patch_install installed in the system, version:pa1
Package : patch_bridge
Status:running
Version: pa1      Build time: Mon May 13 09:03:07 2013
Size: 277        Install time: Tue May 21 03:07:17 2013
Description: a patch for bridge
Required packages: None

```

17.8 show upgrade auto-sync

Use this command to display related auto-sync configuration on the device.

show upgrade auto-sync

**Parameter
Description**

Parameter	Description
N/A	N/A

**Command
Mode**

Privileged EXEC mode

**Default
Level**

2

Usage Guide

This command is used to display the auto-sync upgrade configuration in the system including the policy, range and upgrade package's path.

Prompt

The auto-sync information of the system is displayed after running.

Messages

```

Ruijie#show upgrade auto-sync
auto-sync policy: coordinate
auto-sync range: vsu

```

```
auto-sync package: flash:/eg1000m_main_1.0.0.0f328e91.bin
```

17.9 show upgrade file

Use this command to display the information of the installation package files in the device file system.

show upgrade file *url*

Parameter Description	Parameter	Description
	<i>url</i>	The local <i>url</i> path indicates where an installation package file is stored.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used to preview main messages of an installation package after it is downloaded into local file system.

 This command is not applied to a chassis package.

Configuration The following example displays the information of an installation package file.

Examples

```
Ruijie# show upgrade file flash://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
Name      : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target   : eg1000m
Size             : 26945
Build time       : Wed Dec 7 00:54:56 2013
Install date     : (not installed)
Description      : this is a bridge package
Package files :
  Package files:
    /lib64
    /lib64/libbridge.so
    /sbin
    /sbin/bridge
```

This command is used to obtain the information in the package.

Field	Description
Name	Name of the package
Version	Version of the package
Package type	Type of the package
Support target	Supported product description

Size	Content size of the package
Build time	Compilation time of the package
Install date	Installation time of the package
Description	Description of the package
Package files	All contents in the package

Prompt The package information is displayed after running.

Messages

```
Name      : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target   : eg1000m
Size             : 26945
Build time       : Wed Dec 7 00:54:56 2013
Install date     : (not installed)
Description      : this is a bridge package
Package files :
  Package files:
    /lib64
    /lib64/libbridge.so
    /sbin
    /sbin/bridge
```

17.10 show upgrade history

Use this command to display the upgrade history.

show upgrade history

Parameter Description	Parameter	Description
	N/A	N/A

Command Privileged EXEC mode

Mode

Default Level 2

Configuration The following example displays the upgrade history.

Examples

```
Ruijie#show upgrade history
Last Upgrade Information:
  Time:      2014-08-31 12:15:03
  Method:    LOCAL
Package Name: N18000_RGOS11.0(1)B1_CM_01200616_install.bin
Package Type: Distribution
```

Prompt Messages N/A

Platforms N/A

17.11 show upgrade status

Use this command to display the upgrade status of all line cards on the chassis device.

show upgrade status

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Configuration Examples The following example displays the upgrade status of all line cards on the chassis device.

```
Ruijie#show upgrade status
[slot: M1]
    dev_type: s12k-ppc-cm
    status  : ready
[slot: 8]
    dev_type: s12k-s86-ppc-lc
    status  : upgrading
```

Prompt Messages The upgrade status of various line cards is displayed.

```
[slot: M1]
    dev_type: s12k-ppc-cm
    status  : ready
[slot: 8]
    dev_type: s12k-s86-ppc-lc
    status  : upgrading
```

Platforms

17.12 upgrade

Use this command to install and upgrade an installation package in the local file system.

upgrade [slot {num | M1 | M2 | all }]url[force]

Parameter Description	Parameter	Description
	<i>url</i>	The local path indicates where an installation package is stored. This command is used to upgrade an installation package on the device.
	slot num	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
	slot all	This parameter is used on a chassis device. It indicates all devices including VSU system.
	slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.
	slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.
	force	Mandatory upgrade

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is applicable to installation packages of all subsystem components, chassis devices, feature components and hot patches. Before its use, run the **copy** command to copy feature packages into the file system in the device.

When there is no specified range of parameters, the command is used to upgrade the matched system components according to the auto-sync configuration.

Configuration The following example upgrades the main package on the device.

Examples

```
Ruijie#upgrade usb0:/eg1000m_main_1.0.0.0f328e91.bin
Upgrade processing is 10%
Upgrade processing is 60%
Upgrade processing is 90%
Upgrade info [OK]
Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
Upgrade processing is 100%
Reload system to take effect!
```

The following example upgrades the chassis package on the device.

```
Ruijie# upgrade usb0:/ S8600E_RGOS11.0(4)B1_CM_install.bin
[Slot M1]:Upgrade processing is 10%

[Slot 1]:Upgrade processing is 10%
```



```

[Slot M1]:Upgrade processing is 60%

[Slot 1]:Upgrade processing is 60%

[Slot M1]:Upgrade processing is 90%

[Slot M1]:
Upgrade info [OK]
  Kernel version[2.6.32.abb2b41f170c81->2.6.32.abb2b415749f40]
  Rootfs version[1.0.0.d5f0de03->1.0.0.660e0085]

[Slot M1]:Restart to take effect !

[Slot M1]:Upgrade processing is 100%
[Slot 1]:Upgrade processing is 90%

[Slot 1]:
Upgrade info [OK]
  Kernel version[2.6.32.9f8b56f1d45ab2 ->2.6.32.0f48cb9f170c81]
  Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]

[Slot 1]:Restart to take effect !

[Slot 1]:Upgrade processing is 100%
[slot: M1]
  device_name: ca-octeon-cm
  status:      SUCCESS
[slot: 1]
  device_name: ca-octeon-lc
Status:      SUCCESS

```

Verification Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.

Run the **show component** command to check whether the upgrade of a feature component is successful. upgrading a feature component

Run the **show patch** command to check whether the upgrade of a hot patch is successful.

Prompt The prompt message of successful running is displayed.

Messages Upgrade info [OK]

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade

command.

Device don't support

There is no need to upgrade the device.

The version in device is newer or the same

When there is insufficient space for upgrade, check USB flash disk attached on the device.

No enough space for decompress

Contact the service center to solve the system problem.

No enough space, rootfs been destroyed. Please upgrade in uboot

The existing patch package needs to be uninstalled before upgrade.

Already exist patch, please uninstall before upgrade

The patch package is not applicable to this system and needs to be changed.

Patch compatibility err

The upgrade of a patch package is not available on this device and needs to be regained.

some origin cmpnt has change

17.13 upgrade auto

Use this command to upgrade an installation package automatically without interrupting services on a dual-device VSU system. While either in VSU mode or in standalone mode, one single device will restart after this configuration, thus interrupting services.

upgrade auto *url* [**force**]

Parameter Description	Parameter	Description
	<i>url</i>	Installation package directory
	force	Enforces upgrade.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide Use this command to upgrade the VSU system.
 Download the program of the latest version to the device before running this command (by using the **copy tftp** command).
 During one upgrade, do not use the **upgrade auto** command and other upgrade commands (such as the **upgrade** command) at the same time. If auto-upgrade fails, follow the system prompt to restore

the version.

Do not update the installation package (by running the copy tftp command/U disk copy) or perform other upgrade operation (running the upgrade /upgrade auto command) repetitively.

During auto-upgrade, do not unplug the card, perform hot backup switchover, power off chassis or change VSU software/hardware configuration.

Configuration The following example upgrades the main package automatically without interrupting the service.

Examples

```

2015-04-09_09-56-23 Ruijie#upgrade auto usb0:S6220_RGOS11.0(5)B1_install.bin
2015-04-09_09-56-24 Ruijie#*Jan 1 00:23:40: %7:
2015-04-09_09-56-24 *Jan 1 00:23:40: %7: [Slot 1/0]:Upgrade processing is 10%
2015-04-09_09-56-26 Ruijie#show upgrade status
2015-04-09_09-56-26 [Slot 1/0]
2015-04-09_09-56-26         dev_type: s6k
2015-04-09_09-56-26         status  : upgrading
2015-04-09_09-56-26 [Slot 2/0]
2015-04-09_09-56-26         dev_type: s6k
2015-04-09_09-56-26         status  : transmission
2015-04-09_09-58-20 *Jan 1 00:25:36: %7: [Slot 2/0]:Upgrade processing is 10%
2015-04-09_09-58-30 Ruijie#show upgrade status
2015-04-09_09-58-30 [Slot 1/0]
2015-04-09_09-58-30         dev_type: s6k
2015-04-09_09-58-30         status  : upgrading
2015-04-09_09-58-30 [Slot 2/0]
2015-04-09_09-58-30         dev_type: s6k
2015-04-09_09-58-30         status  : upgrading
2015-04-09_09-58-39 *Jan 1 00:25:56: %7:
2015-04-09_09-58-39 *Jan 1 00:25:56: %7: [Slot 2/0]:Upgrade processing is 60%
2015-04-09_09-59-19 *Jan 1 00:26:35: %7:
2015-04-09_09-59-19 *Jan 1 00:26:35: %7: [Slot 2/0]:Upgrade processing is 90%
2015-04-09_09-59-19 *Jan 1 00:26:35: %7:
2015-04-09_09-59-19 *Jan 1 00:26:35: %7: [Slot 2/0]:
2015-04-09_09-59-19 *Jan 1 00:26:35: %7: Upgrade info [OK]
2015-04-09_09-59-19 *Jan 1 00:26:36: %7:   Kernel
version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_09-59-19 *Jan 1 00:26:36: %7:   Rootfs
version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_09-59-19 *Jan 1 00:26:36: %7:
2015-04-09_09-59-19 *Jan 1 00:26:36: %7: [Slot 2/0]:Reload system to take
effect!
2015-04-09_09-59-21 *Jan 1 00:26:37: %7:
2015-04-09_09-59-21 *Jan 1 00:26:37: %7: [Slot 2/0]:Upgrade processing is 100%
2015-04-09_10-00-28 Ruijie#show upgrade status
2015-04-09_10-00-28 [Slot 1/0]
2015-04-09_10-00-28         dev_type: s6k

```

```
2015-04-09_10-00-28      status  : upgrading
2015-04-09_10-00-28 [Slot 2/0]
2015-04-09_10-00-28      dev_type: s6k
2015-04-09_10-00-28      status  : success
2015-04-09_10-01-39 *Jan  1 00:28:56: %7:
2015-04-09_10-01-39 *Jan  1 00:28:56: %7: [Slot 1/0]:Upgrade processing is 60%
2015-04-09_10-02-17 *Jan  1 00:29:33: %7:
2015-04-09_10-02-17 *Jan  1 00:29:33: %7: [Slot 1/0]:Upgrade processing is 90%
2015-04-09_10-02-17 *Jan  1 00:29:33: %7:
2015-04-09_10-02-17 *Jan  1 00:29:33: %7: [Slot 1/0]:
2015-04-09_10-02-17 *Jan  1 00:29:34: %7: Upgrade info [OK]
2015-04-09_10-02-17 *Jan  1 00:29:34: %7:   Kernel
version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_10-02-17 *Jan  1 00:29:34: %7:   Rootfs
version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_10-02-17 *Jan  1 00:29:34: %7:
2015-04-09_10-02-18 *Jan  1 00:29:34: %7: [Slot 1/0]:Reload system to take
effect!
2015-04-09_10-02-19 *Jan  1 00:29:35: %7:
2015-04-09_10-02-19 *Jan  1 00:29:35: %7: [Slot 1/0]:Upgrade processing is 100%
2015-04-09_10-02-19 *Jan  1 00:29:36: %7: %PKG_MGMT:auto-sync config
synchronization, Please wait for a moment....
2015-04-09_10-02-20 *Jan  1 00:29:36: %7:
2015-04-09_10-02-20 [ 1784.116069] rtc-pcf8563 6-0051: retrieved date/time is
not valid.
2015-04-09_10-02-20 *Jan  1 00:29:36: %7: [Slot 2/0]:auto sync config: space
not enough left 57229312, need 114597815
2015-04-09_10-02-20 *Jan  1 00:29:36: %7:
2015-04-09_10-02-20 *Jan  1 00:29:36: %7: [Slot 2/0]:auto sync package config
err
2015-04-09_10-02-20 *Jan  1 00:29:37: %7: [Slot 1/0]
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   device_name: s6k
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   status:      SUCCESS
2015-04-09_10-02-21 *Jan  1 00:29:37: %7: [Slot 2/0]
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   device_name: s6k
2015-04-09_10-02-21 *Jan  1 00:29:37: %7:   status:      SUCCESS
2015-04-09_10-02-21 *Jan  1 00:29:38: %7: %Do with dtm callback....
2015-04-09_10-02-21 *Jan  1 00:29:38: %VSU-5-DTM_AUTO_UPGRADE:
Upgrading the system, wait a moment please.
```

17.14 upgrade auto-sync package

Use this command to configure the path for the auto-sync upgrade.

upgrade auto-sync package *url*

Parameter Description	Parameter	Description
	<i>url</i>	The path of installation package.

Defaults The default is the last upgrade path.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide It is recommended to use default settings.

Configuration The following example sets the path to the upgrade package in the USB flash disk.

Examples Ruijie# upgrade auto-sync package usb0:/eg1000m_main_1.0.0.0f328e91.bin

Verification Run the **show upgrade auto-sync** command to display current auto-sync policy.
If *url* provides normal path, run the **stat** command to check whether it can be accessed.

Prompt Messages The prompt message of successful running is displayed:

```
Upgrade auto-sync package is set as usb0:/eg1000m_main_1.0.0.0f328e91.bin
```

17.15 Upgrade auto-sync policy

Use this command to set an auto-sync policy for the system.

upgrade auto-sync policy [**none** | **compatible** | **coordinate**]

Parameter Description	Parameter	Description
	none	No auto-sync upgrade
	compatible	Performs auto-synchronization based on the sequential order of versions.
	coordinate	Synchronizes with the version based on the system upgrade patch stored on the supervisor module.

Defaults **coordinate**

Command Mode	Privileged EXEC mode
Default Level	2
Usage Guide	Check whether the upgrade package is ready before using the command.
Configuration Examples	The following example sets the auto-sync policy of the device based on the version of supervisor modules.
	<pre>Ruijie# upgrade auto-sync policy coordinate</pre>
Verification	Display the current policy for auto-sync upgrade by running the show upgrade auto-sync command.
Prompt Messages	The prompt message of successful running is displayed.
	<pre>Upgrade auto-sync policy is set as coordinate.</pre>

17.16 upgrade auto-sync range

Use this command to set the range of auto-sync upgrade.

upgrade auto-sync range [chassis | vsu]

Parameter Description	Parameter	Description
	chassis	Auto-sync version upgrade in the range of chassis
	vsu	Auto-sync version upgrade in the range of the VSU system.

Defaults	vsu
Command Mode	Privileged EXEC mode
Default Level	2
Usage Guide	It is recommended to set the parameter to vsu to ensure system version consistency to the most extent.
Configuration Examples	The following example installs the auto-sync upgrade in the VSU system.
	<pre>Ruijie# upgrade auto-sync range vsu</pre>
Verification	Run the show upgrade auto-sync command to display the range of current auto-sync upgrade.
Prompt Messages	The prompt message of successful running is displayed.
	<pre>Upgrade auto-sync range is set as vsu.</pre>

17.17 upgrade download tftp

Use this command to download, install and upgrade installation packages from the tftp server.

upgrade download tftp:*path* [**force**]

upgrade download oob_tftp:*path*[**via mgmt** {*number*}] [**force**]

Parameter Description	Parameter	Description
	<i>path</i>	The path of installation packages on the tftp server This command is downloaded and upgraded automatically from the server.
	via mgmt <i>number</i>	If the transfer mode is <i>oob_tftp</i> and there are multiple MGMT ports, you can select a specific port.
	force	Enforces upgrade.

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is applicable to installation packages of all subsystem components, chassis devices, feature components and hot patches. This command is used to perform automatic installation, copy and upgrade of files.

Configuration The following example upgrades the main package.

```

Examples
Ruijie# upgrade download
tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
Upgrade processing is 10%
Upgrade processing is 60%
Upgrade processing is 90%
Upgrade info [OK]
      Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
      Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
Upgrade processing is 100%
Reload to take effect!
    
```

Verification Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.

Run the **show component** command to check whether the upgrade of a feature component is successful.

Run the **show patch** command to check whether the upgrade is successful of a hot patch package.

Prompt

The prompt message of successful running is displayed.

Messages

```
Upgrade info [OK];
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

The existing patch package needs to be deleted.

```
Already exist patch, please uninstall before upgrade
```

The patch package is not compatible on this device. Replace the package..

```
Patch compatibility err
```

The upgrade of the patch package is not applied to the device. Regain the package.

```
Some origin component has change
```

17.18 upgrade rollback

Use this command to roll a subsystem back to the version before the upgrade.

```
upgrade rollback [ slot {num | M1 | M2 | all } ]
```

**Parameter
Description**


Parameter	Description
slot num	This parameter is used on a chassis device. It indicates a corresponding line card based on the slot number.
slot all	This parameter is used on a chassis device. It indicates all devices.
slot M1	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M1.

slot M2	This parameter is used on a chassis device. It specifies that the operation is performed on supervisor module M2.
----------------	---

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used when the device cannot work properly after subsystem upgrade. It takes effect only when the last upgrade of subsystem components is successful.

 The command is valid after device restart. The recursive rollback cannot be executed through this command in succession.

Configuration Examples The following example rolls a subsystem back to the version before the upgrade on the box device.

```
Ruijie#upgrade rollback
kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21] [OK]
rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537] [OK]
Rollback success!
Reload system to take effect!
```

The following example rolls a subsystem back to the version before the upgrade on the chassis device.

```
Ruijie#upgrade rollback slot M1
[Slot M1]:
kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21] [OK]
rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537] [OK]
Rollback success!
Reload system to take effect!
```

Verification Run the **show version detail** command to check the result of rolling back subsystem components after device restart.

Prompt Messages The prompt message of successful running is displayed.

```
Rollback success!
Restart to take effect !
```

The rollback operation cannot be performed when subsystem components have not been upgraded last time.

```
Not subsys package last upgrade
```

The rollback operation cannot be performed for the last upgrade is not successful.

```
Last upgrade error skip
```

The upgrade command has not been run or the rollback operation has been performed.

```
Monitor file lost
```

Common Errors The last upgrade is not for subsystem components, but for feature packages, hot patch packages and so on.
Run the rollback command for subsystem once.

18 OpenFlow Commands

18.1 of controller-ip

Use this command to enable OpenFlow.

of controller-ip *ip-address* [**port** *port-id*] **interface** [*interface-id*]

Use the **no** form of this command to disable OpenFlow.

no of controller-ip [*ip-address*]

Parameter Description	Parameter	Description
	<i>ip-address</i>	Controller IP address. If you configure the no form of this command without any parameter, all controllers are disabled. (OpenFlow1.0 supports connection to one single controller).
	port <i>port-id</i>	Controller access port ID. The default for OpenFlow1.0 is 6633.
	Interface <i>interface-id</i>	Interface ID, whether out-of-band MGMT interface or in-band physical port (some devices may not have MGMT interfaces).

Command Mode Global configuration mode

Default OpenFlow is disabled by default.

Usage Guide N/A

Configuration The following example enables OpenFlow.

Examples

```
Ruijie (config)#of controller-ip 192.168.21.57 interface gigabitEthernet 0/1
The following example disables OpenFlow.
Ruijie#no of controller-ip
```

18.2 of mode

Use this command to configure the controller mode.

of mode [**single** | **multiple**]

Use the **no** form of this command to restore the default setting.

no of mode

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Global configuration mode

Default The default mode is multiple.

Usage Guide Configure this command before enabling the controller.

Configuration The following example enables the single mode.

Examples

```
Ruijie(config)#of mode single
```

The following example enables the multiple mode.

```
Ruijie(config)#of mode multiple
```

The following example restores the default setting.

```
Ruijie(config)#no of mode
```

18.3 of packet table-lookup

Use this command to enable table-lookup mode or disable table-lookup mode.

of packet table-lookup [enable | disable]

no of packet table-lookup

Parameter	Parameter	Description
Description	N/A	N/A

Command Mode Global configuration mode

Default The table-lookup mode is enabled by default.

Usage Guide N/A

Configuration The following example enables the table-lookup mode.

Examples

```
Ruijie(config)#of packet table-lookup enable
```

The following example disables the table-lookup mode.

```
Ruijie(config)#of packet table-lookup disable
```

The following example restores the default setting.

```
Ruijie(config)#no of packet table-lookup
```

18.4 of packet vlantag

Use this command to determine whether to contain the VLAN tag in the packet sent by the OpenFlow device.

[no] of packet vlantag

Parameter	Parameter	Description
Description	N/A	N/A

Command Mode Global configuration mode

Default The VLAN tag is contained in the packet sent by the OpenFlow device by default.

Usage Guide N/A

Configuration The following example contains the VLAN tag in the packet sent by the OpenFlow device.

Examples

```
Ruijie(config)#of packet vlantag
```

The following example does not contain the VLAN tag in the packet sent by the OpenFlow device..

```
Ruijie(config)#no of packet vlantag
```

18.5 of source-ip

Use this command to configure the source IP address of the controller.

of source-ip

Parameter Description	Parameter	Description
	<i>ip-address</i>	Source IP address

Command Mode Global configuration mode

Default The default source IP address is the interface IP address.

Usage Guide N/A

Configuration The following example configures the source IP address of the controller.

Examples

```
Ruijie(config)#of source-ip 192.168.197.25
```

18.6 show of

Use this command to display the connection between the current device and the controller.

show of

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Global configuration mode

Default N/A

Usage Guide Use this command to display the OpenFlow version on the device.

Configuration The following example displays the connection between the current device and the controller.

Examples `Ruijie#show of`

18.7 show of flowtable

Use this command to display flow table entries of OpenFlow Device

show of flowtable

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Global configuration mode

Default N/A

Usage Guide Running the **of controller-ip** command before configuring this command. Otherwise, the flow table entries are not displayed.

Configuration The following example display flow table entries.

Examples `Ruijie#show of flowtable`

18.8 show of port

Use this command to display port information of OpenFlow device.

show of port

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Global configuration mode

Default N/A

Usage Guide Running the **of controller-ip** command before configuring this command. Otherwise, the port information is not displayed.

Configuration The following example displays port information of OpenFlow device.

Examples `Ruijie#show of port`



Ethernet Switch Commands

1. Interface Commands
2. MAC Address Commands
3. Aggregate Port Commands
4. VLAN Commands
5. MAC VLAN Commands
6. Super-VLAN Commands
7. Protocol VLAN Commands
8. Private VLAN Commands
9. Voice VLAN Commands
10. MSTP Commands
11. GVRP Commands
12. LLDP Commands
13. QinQ Commands
14. ERPS Commands

1 Interface Commands

1.1 bandwidth

Use this command to set the bandwidth on the interface. Use the **no** form of this command to restore the default setting.

bandwidth *kilobits*
no bandwidth

Parameter Description	Parameter	Description
	<i>kilobits</i>	Bandwidth per second, in the unit of Kbps.

Defaults If this command is not configured on the interface, use the show interface command to display the default setting in privileged EXEC mode.

Command Mode Interface configuration mode

Usage Guide This command does not affect the actual bandwidth on the interface. Instead, it is used to display the system the bandwidth specification. By default, the bandwidth is determined by the actual link rate on the interface. It can be set by the user as well.

Configuration Examples The following example sets the bandwidth on the interface to 64 Kbps.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# bandwidth 64
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.2 carrier-delay

Use this command to set the carrier delay on the interface. Use the no form of this command to restore the default value.

carrier-delay { [milliseconds] num | up [milliseconds] num down [milliseconds] num}
no carrier-delay

Parameter Description	Parameter	Description
	num	(Optional) in the range from 0 to 60 in the unit of seconds.
	milliseconds	(Optional) in the range from 0 to 60000 in the unit of milliseconds.
	up	(Optional) Configures the delay after which DCD changes from Down to Up in status.
	down	(Optional) Configures the delay after which DCD changes from Up to Down in status.

Defaults The default is 2 seconds.

Command Mode Interface configuration mode

Usage Guide This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status or vice versa. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation. If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.

Configuration Examples The following example sets the carrier delay of serial interface to 5 seconds.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config)# carrier-delay 5
```

The following example sets the carrier delay of serial interface to 100 milliseconds.

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)#carrier-delay milliseconds 100
```

The following example sets the DCD delay from Down to Up in status to 100 milliseconds and from Up to Down to 200 milliseconds.

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# carrier-delay up milliseconds 100 down
milliseconds 200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.3 clear counters

Use this command to clear the counters on the specified interface.

clear counters [*interface-id*]

Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

Configuration Examples The following example clears the counters on interface gigabitethernet 1/1.

```
Ruijie# clear counters gigabitethernet 1/1
```

Related Commands	Command	Description
	show interfaces	Displays the interface information.

Platform Description N/A

1.4 clear interface

Use this command to reset the interface.

clear interface *interface-id*

Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command is only used on the switch port, member port of the L2 Aggregate port, routing port,

and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

Configuration The following example resets the interface gigabitethernet 1/1.

Examples

```
Ruijie# clear interface gigabitethernet 1/1
```

**Related
Commands**

Command	Description
shutdown	Disables the interface.

Platform N/A

Description

1.5 description

Use this command to configure the alias of interface. Use the **no** form of this command to restore the default setting.

description *string*

no description

**Parameter
Description**

Parameter	Description
<i>string</i>	Interface alias

Defaults No alias is configured by default.

**Command
Mode** Interface configuration mode.

Usage Guide Use **show interfaces** to display the interface information, including the alias.

Configuration The following example configures the alias of interface.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# description GBIC-1
```

**Related
Commands**

Command	Description
show interfaces	Displays the interface information.

Platform N/A

Description

1.6 duplex

Use this command to specify the duplex mode for the interface. Use the **no** form of this command to restore the default setting.

duplex { **auto** | **full** | **half** }

no duplex

Parameter Description

Parameter	Description
auto	Self-adaptive full duplex and half duplex
full	Full duplex
half	Half duplex

Defaults The default is **auto**,

Command Interface configuration mode.

Mode

Usage Guide The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

Configuration The following example specifies the duplex mode for the interface.

Examples

```
Ruijie(config-if)# duplex full
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform N/A

Description

1.7 errdisable recovery

Use this command to recover the interface in violation.

errdisable recovery [**interval** *time*]

Parameter Description

Parameter	Description
<i>time</i>	Time for the command to take effect. The range is from 30 to 86,400 seconds.

Defaults N/A

Command Interface configuration mode.
Mode

Usage Guide Use the command to recover the port that triggers violation after being configured with the **violation shutdown** command.

Configuration The following example recovers the violation interface gigabitethernet 1/1.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# errdisable recovery
```

Related Commands

Command	Description
switchport port-security violation shutdown	Configures the port security violation to shutdown.

Platform N/A.

Description

1.8 flowcontrol

Use this command to enable or disable the flow control. Use the **no** form of this command to restore the default setting.

flowcontrol { auto | off | on }
no flowcontrol

Parameter Description

Parameter	Description
auto	Self-negotiates the flow control.
off	Disables the flow control.
on	Enables the flow control.

Defaults This function is disabled by default.

Command Interface configuration mode.
Mode

Usage Guide Use the **show interfaces** command to display the flow control configuration.

Configuration The following example enables flow control on fastEthernet port 1/1.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# flowcontrol on
```

Related

Command	Description
---------	-------------

Commands	
show interfaces	Displays the interface information.

Platform N/A

Description

1.9 interface

Use this command to enter the interface configuration mode.

interface *interface-type interface-number*

Parameter Description	Parameter	Description
	<i>interface-type</i>	The interface type.
	<i>interface-number</i>	The interface ID.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is used to enter interface configuration mode. The user can modify the interface configuration next,

Configuration Examples The following example enters configuration mode on Aggregateport 1.

```
Ruijie(config)# interface Aggregateport 1
Ruijie(config-if-Aggregateport 1)#
```

The following example enters configuration mode on GigabitEthernet 1/2.

```
Ruijie(config)# interface GigabitEthernet 1/2
Ruijie(config-if-GigabitEthernet 1/2)#
```

The following example configuration mode on VLAN 1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)#
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.10 interface range

Use this command to enter interface configuration mode on multiple interfaces.

interface range { *port-range* | **macro** *macro_name* }

Use this command to define the macro name of the **interface range** command.

define interface-range *macro_name*

Parameter Description	Parameter	Description
	<i>port-range</i>	The interface type and ID range, entered in the form of <i>interface-type slot-number/interface-number</i> . The interface can be either an Ethernet physical interface or a loopback interface.
	macro <i>macro_name</i>	The macro name which represents the interface range.

Defaults The **interface range** command is disabled by default.

Command Global configuration mode

Mode

Usage Guide Use the **define interface-range** command to define a range of interfaces as the macro name and then use the **interface range macro macro_name** command to enter interface configuration mode on multiple interfaces.

Configuration Examples The following example enters interface configuration mode on multiple interfaces by setting the interface range.

```
Ruijie(config)# interface range gigabitEthernet 0/0, 0/2
Ruijie(config-if-range)# bandwidth 100
```

The following example enters interface configuration mode on multiple interfaces by defining the macro name.

```
Ruijie(config)# define interface-range routel gigabitEthernet 0/0-2
Ruijie(config)# interface range macro routel
Ruijie(config-if-range)# bandwidth 100
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.11 line-detect

Use this command to detect the cable connection status.

line-detect

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide This command is used to detect the line status and locate the problem in case of a line failure, for example, the line is torn down.

Configuration Examples The following example detects the cable connection status on gigabitEthernet 0/1.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#line-detect

Interface : GigabitEthernet 0/1
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state      length(meters)
-----
A   Ok          1
pair state      length(meters)
-----
B   Ok          2
pair state      length(meters)
-----
C   Short       1
pair state      length(meters)
-----
D   Short       1
```

Field	Description
pairs	Number of line pairs included. For example, the twisted pair includes four pairs of lines.
state	Status of the current line pair: OK, Short or Open. In general, the 100M twisted pairs A and B are OK, C and D are Short. The 1000M twisted pairs A, B, C and D are all OK.

length	Length of the line in meter. Only the length of the line pair whose status is OK takes effect. Since the length is calculated based on the transmission time of signal, there may have a certain difference. The length of the line pair whose status is Short or Open is the length from the port to the faulty point.
--------	---

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.12 load-interval

Use this command to set the interval for calculating load on the interface. Use the **no** form of this command to restore the default setting.

load-interval *seconds***no load-interval****Parameter Description**

Parameter	Description
<i>seconds</i>	In the range from 5 to 600 in the unit of seconds.

Defaults The default is 10.**Command Mode** Interface configuration mode

Usage Guide This command is used to set the interval for calculating load on the interface. In general, the numbers of incoming and outgoing packets and bytes are calculated every 10 seconds. For example, if the parameter is set to 180 seconds, the following outcome is displayed when the **show interface gigabitEthernet 0/1** command is run.

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

Configuration Examples The following example sets the interval for calculating load on interface GigabitEthernet 0/1 to 180 seconds.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# load-interval 180
```

Related Commands

Command	Description
---------	-------------

N/A	N/A
-----	-----

Platform N/A

Description

1.13 logging

Use this command to print information on the interface. Use the **no** form of this command to disable this function.

logging [**link-updown** | **error-frame** | **link-dither**]

no logging [**link-updown** | **error-frame** | **link-dither**]

Parameter Description	Parameter	Description
	link-updown	Prints the status change information.
	error-frame	Prints the error frame information.
	link-dither	Prints the oscillation information.

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example prints information on the interface..

```
Ruijie(config)# logging link-updown
Ruijie(config)# logging error-frame
Ruijie(config)# logging link-dither
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.14 medium-type

Use this command to specify the medium type for an interface. Use the **no** form of this command to restore the default setting.

medium-type { **auto-select** [**prefer** [**fiber** | **copper**]] | **fiber** | **copper** }

no medium-type

Parameter Description	Parameter	Description
	fiber	Optical interface.
	prefer [fiber copper]	The preferred medium type for the interface is selected.
	auto-select	Auto-selects the medium type for the interface.
	copper	Copper interface.

Defaults The default is **copper**.

Command Mode Interface configuration (physical interface, except for AP and SVI)

Usage Guide If a port can be selected as an optical port or electrical port, you can only select one of them. Once the media type is selected, the attributes of the port, for example, status, duplex, flow control, and rate, all mean those of the currently selected media type. After the port type is changed, the attributes of the new port type take the default values, which can be modified as needed.

Configuration Examples The following example specifies the medium type for interface gigabitethernet 1/1.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# medium-type copper
```

Related Commands	Command	Description
	show interfaces	Displays the interface information.

Platform Description The 12 SFP interfaces of the 24SFP/12GT line cards and 1210/100/1000M BASE-T interfaces allow for dynamic switching.

The combo interface is not supported to automatically determine whether the current port is the SFP interface or the 10/100/1000M BASE-T interface.

1.15 mtu

Use this command to set the MTU supported on the interface.

mtu *num*

Parameter Description	Parameter	Description
	<i>num</i>	64 to 9216 (or 65536, which varies by products)

Defaults The default is 1500.

Command Interface configuration mode.

Mode

Usage Guide This command is used to set the maximum transmission unit (MTU) supported on the interface.

Configuration The following example sets the MTU supported on interface `gigabitethernet 1/1` to 9000.

Examples

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet)# mtu 9000
```

**Related
Commands**

Command	Description
show interfaces	Displays the interface information.

Platform N/A

Description

1.16 negotiation mode

Use this command to enable or disable auto-negotiation mode. Use the **no** form of this command to restore the default setting.

negotiation mode { on | off }

no negotiation mode

**Parameter
Description**

Parameter	Description
on	Enables auto-negotiation.
off	Disables auto-negotiation.

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide In general, the auto-negotiation status is determined by interface speed, duplex, flow control and auto-negotiation factor mode.

Configuration The following example enables auto-negotiation mode on interface `GigabitEthernet 1/1`.

Examples

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# negotiation mode on
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

1.17 physical-port dither protect

Use this command to enable oscillation protection on the port. Use the **no** form of this command to disable this function.

physical-port dither protect

no physical-port dither protect

**Parameter
Description**


Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Global configuration mode

Mode

Usage Guide After you configure the **physical-port dither protect** command, the port will be shut down when the oscillation occurs for certain times.

 If oscillation occurs on the port for 6 times within 2 seconds, a syslog will be printed. If syslog is printed for 10 consecutive times, the port will be shut down, If oscillation occurs on the port for over 10 times within 10 seconds, a syslog will be printed but the port will not be shut down.

Configuration The following example enables oscillation protection on the port.

Examples

```
Ruijie(config)# physical-port dither protect
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

1.18 protected-ports route-deny

Use this command to configure L3 routing between the protected ports. Use the **no** form of this command to restore the default setting.

protected-ports route-deny

no protected-ports route-deny

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default..	
Command Mode	Global configuration mode.	
Usage Guide	The ports that are set as the protected ports can route on L3. Use this command to deny the L3 communication between protected ports. Use the show running-config command to display configuration.	
Configuration Examples	The following example configures L3 routing between the protected ports.	
Examples	<pre>Ruijie(config)# protected-ports route-deny</pre>	
Related Commands	Command	Description
	show running-config	Displays the protected ports route-deny configuration.
Platform Description	N/A	

1.19 show interfaces

Use this command to display the interface information and optical module information.

show interfaces [*interface-type interface-number*] [**description** | **switchport** | **trunk**]

Parameter Description	Parameter	Description
	<i>interface-id</i> <i>interface-number</i>	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
	description	The description of the interface, including the link status.
	switchport	Layer 2 interface information.
	trunk	Trunk port, applicable for physical port and aggregate port.

Defaults	All interface information is displayed by default.
Command Mode	Privileged EXEC mode.
Usage Guide	This command is used to show all basic information if no parameter is specified.

Configuration The following example displays the interface information when the Gi0/1 is a Trunk port.

Examples

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
  flow receive control admin status is OFF,flow send control admin status is OFF,flow
  receive control oper status is Unknown,flow send control oper status is Unknown
  broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
  is OFF
  Port-type: trunk
  Native vlan:1
  Allowed vlan lists:1-4094
  Active vlan lists:1, 3-4
    5 minutes input rate 0 bits/sec, 0 packets/sec
    5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
```

The following example displays the interface information when the Gi0/1 is an Access port.

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
```



```
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow receive control admin status is OFF,flow send control admin status is
  OFF,flow receive control oper status is Unknown,flow send control oper status is
  Unknown
  broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
  is OFF
  Port-type: access
  Vlan id : 2
    5 minutes input rate 0 bits/sec, 0 packets/sec
    5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
```

The following example displays the layer-2 interface information when the Gi0/1 is a Hybrid port.

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
```

```

Input queue 0/75, 0 drops
Switchport attributes:
  interface's description:""
  medium-type is copper
  lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
  Priority is 0
  admin duplex mode is AUTO, oper duplex is Unknown
  admin speed is AUTO, oper speed is Unknown
  flow receive control admin status is OFF,flow send control admin status is
OFF,flow receive control oper status is Unknown,flow send control oper status is
Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: hybrid
Tagged vlan id:2
Untagged vlan id:none
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets

```

The following example displays the layer-2 information of the Gi0/1.

```

Ruijie# show interfacesgigabitEthernet 0/1 switchport
Interface Switchport ModeAccess Native Protected VLAN lists
-----
GigabitEthernet 0/1 enabled Access 11 Disabled ALL

```

Related Commands

Command	Description
duplex	Duplex
flowcontrol	Flow control status.
interface gigabitEthernet	Selects the interface and enter the interface configuration mode.
interface aggregateport	Creates or accesses the aggregate port, and enters the interface configuration mode.
interface vlan	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
shutdown	Disables the interface.
speed	Configures the speed on the port.
switchport priority	Configures the default 802.1q interface priority.

switchport protected	Configures the interface as a protected port.
-----------------------------	---

Platform N/A

Description

1.20 show interfaces counters

Use this command to display the received and transmitted packet statistics.

show interfaces [*interface-type interface-number*] **counters** [**increment** | **error** | **rate** | **summary**]
[*up* | *down*]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	(Optional) The interface type and ID.
	increment	Displays the packet statistics increased during the last sample interval.
	error	Displays error packet statistics.
	rate	Displays packet receiving and transmitting rate.
	summary	Displays packet statistics summary.
	<i>up</i>	(Optional) Displays the port up statistics.
	<i>down</i>	(Optional) Displays the port down statistics.

Defaults N/A

Command Mode Any CLI mode

Usage Guide If you do not specify an interface, the packet statistics on all interfaces are displayed.

Configuration Examples The following example displays packet statistics on interface GigabitEthernet 0/1.

```
Ruijie#show interfaces GigabitEthernet 0/1 counters
Interface : GigabitEthernet 0/1
5 minute input rate : 9144 bits/sec, 9 packets/sec
5 minute output rate : 1280 bits/sec, 1 packets/sec
Rxload           : 1%
InOctets         : 17310045
InPkts          : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
InUcastPkts     : 100
InMulticastPkts : 100
InBroadcastPkts : 800
Txload          : 1%
OutOctets       : 1282535
```

```

OutPkts          : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts     : 100
OutMulticastPkts : 100
OutBroadcastPkts : 800
Undersize packets : 0
Oversize packets : 0
collisions       : 0
Fragments        : 0
Jabbers          : 0
CRC alignment errors : 0
AlignmentErrors  : 0
FCSErrors        : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64:46264
  65-127: 47427
  128-255: 3478
  256-511: 658
  512-1023: 18016
  1024-1518: 125
Packet increment in last sampling interval(5 seconds):
  InOctets       : 10000
  InPkts         : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts    : 100
  InMulticastPkts : 100
  InBroadcastPkts : 800
  OutOctets      : 10000
  OutPkts        : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  OutUcastPkts   : 100
  OutMulticastPkts : 100

```

- i** Rxload refers to the receive bandwidth usage and Txload refers to the Tx bandwidth usage. InPkts is the total number of receive unicast, multicast and broadcast packets. OutPkts is the total number of transmit unicast, multicast and broadcast packets.
- Packet increment in last sampling interval (5 seconds) represents the packet statistics increased during the last sample interval (5 seconds).

The following example displays the packet statistics on interface GigabitEthernet 0/1 increased during the last sample interval.

```

Ruijie#show interfaces GigabitEthernet 0/1 counters increment
Interface : GigabitEthernet 0/1
Packet increment in last sampling interval(5 seconds):
  InOctets       : 10000
  InPkts         : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts    : 100

```

```
InMulticastPkts      : 100
InBroadcastPkts     : 800
OutOctets           : 10000
OutPkts             : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts       : 100
OutMulticastPkts    : 100
```

The following example displays error packet statistics on interface GigabitEthernet 0/1.

```
Ruijie#show interfaces GigabitEthernet 0/1 counters increment
Interface      UnderSize      OverSize      Collisions
Fragments
-----
-----
Gi0/1          0              0              0              0
Interface      Jabbers        CRC-Align-Err  Align-Err
FCS-Err
-----
-----
Gi0/1          0              0              0              0
```

- i** UnderSize is the number of valid packets smaller than 64 bytes.
- OverSize is the number of valid packets smaller than 1518 bytes.
- Collisions is the number of colliding transmit packets.
- Fragments is the number of packets with CRC error or frame alignment error which are smaller than 64 bytes.
- Jabbers is the number of packets with CRC error or frame alignment error which are smaller than 1518 bytes.
- CRC-Align-Err is the number of receive packets with CRC error.
- Align_Err is the number of receive packets with frame alignment error.
- FCS-Err is the number of receive packets with FCS error.

The following example displays packet receiving and transmitting rate on interface GigabitEthernet 0/1.

```
Ruijie#show interface gigabitEthernet 0/1 counters rate
Interface      Sampling Time      Input Rate      Input Rate
Output Rate      Output Rate
                  (bits/sec)      (packets/sec)
(bits/sec)      (packets/sec)
-----
-----
Gi0/1          5 seconds          23391           23              124
0
```

- i** Sampling Time is the time when packets are sampled. Input rate is packet receiving rate and Output rate is packet transmitting rate.

The following example displays packet statistics summary on interface GigabitEthernet 0/1.

```
Ruijie#show interface gigabitEthernet 0/1 counters summary
```

Interface	InOctets	InUcastPkts	InMulticastPkts	InBroadcastPkts

Gi0/1	1475788005	1389	45880503	11886621
Interface	OutOctets	OutUcastPkts	OutMulticastPkts	OutBroadcastPkts

Gi0/1	6667915	6382	31629	13410

i InOctets is the total number of packets received on the interface. InUcastPkts is the number of unicast packets received on the interface. InMulticastPkts is the number of multicast packets received on the interface. InBroadcastPkts is the number of broadcast packets received on the interface.

OutOctets is the total number of packets transmitted on the interface. OutUcastPkts is the number of unicast packets transmitted on the interface. OutMulticastPkts is the number of multicast packets transmitted on the interface. OutBroadcastPkts is the number of broadcast packets transmitted on the interface.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.21 show interfaces counters rate physical-layer

Use this command to packet rate count on the physical layer.

show interfaces [*interface-type interface-number*] **counters rate physical-layer**

Parameter Description

Parameter	Description
<i>interface-type</i>	The interface type and ID. The default is all interfaces.
<i>interface-number</i>	

Defaults

N/A

Command Mode

Any CLI Mode

Usage Guide

If you do not specify an interface, the link state statistics of all interfaces are displayed.

Configuration The following example displays the rate statistics of interface TenGigabitEthernet 0/1.

Examples

```
Ruijie(config-if-TenGigabitEthernet 0/1)#show interface tenGigabitEthernet
0/1 counters rate physical-layer
Interface      Sampling Time      Input Rate          Input Rate
Output Rate    Output Rate
                (bits/sec)         (packets/sec)
(bits/sec)     (packets/sec)
-----
Te0/1          5 seconds          655557576           301267
655557132
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

1.22 show interfaces link-state-change statistics

Use this command to display the link state change statistics, including the time and count.

show interfaces [*interface-type interface-number*] **link-state-change statistics**

Parameter Description

Parameter	Description
<i>interface-type</i>	The interface type and ID.
<i>interface-number</i>	

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the link state statistics of all interfaces are displayed.

Configuration The following example displays the link state statistics of interface GigabitEthernet 0/1.

Examples

```
Ruijie# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface      Link state      Link state change times      Last change time
-----
-----
```

Gi 0/1	down	100	2012-12-24 15:00:00
Interface		Description	
Link state		Current link state.	
Link state change times		The count of link state change.	
Last change time		The time when the last link state change occurs.	

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

1.23 show interfaces status

Use this command to display interface status information.

show interfaces [*interface-type interface-number*] **status**

Parameter Description

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	The interface type and ID.
status	Displays interface status information, including speed and duplex.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the status information of all interfaces is displayed.

Configuration Examples The following example displays the status information of interface GigabitEthernet 0/1.

Examples

```
Ruijie#show interfaces GigabitEthernet 0/1 status
Interface          Status      Vlan    Duplex  Speed  Type
-----
GigabitEthernet 0/1  up         1       Full   1000M  copper
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.24 show interfaces status err-disable

Use this command to display the interface violation status.

show interfaces [*interface-type interface-number*] **status err-disable**

Parameter Description	Parameter	Description
	<i>interface-type</i>	(Optional) The interface type and ID.
	<i>interface-number</i>	


Defaults

Command Mode Any CLI mode

Usage Guide If you do not specify an interface, violation status of all interfaces is displayed.

Configuration Examples The following example displays the violation status of interface GigabitEthernet 0/1.

```
Ruijie#show interface gigabitEthernet 0/1 status err-disabled
Interface                Status          Reason
-----
GigabitEthernet 0/1      err-disabled    BPDU Guard
```

 The violation status is displayed as **err-disabled**.

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.25 show interfaces transceiver

Use this command to display transceiver information of the interface.

show interfaces [*interface-type interface-number*] **transceiver** [**alarm** | **diagnosis**]

Parameter Description	Parameter	Description
	<i>interface-type</i>	The interface type and ID.

<i>interface-number</i>	
transceiver	Displays the transceiver information.
alarm	Displays the alarm message of the transceiver. If there is no alarm message, it is displayed as None.
diagnosis	Displays the diagnostic parameters of the transceiver.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide If you do not specify an interface, the transceiver information of all interfaces is displayed.

Configuration The following example displays the transceiver information of interface GigabitEthernet 5/4.

Examples

```
Ruijie#show interfaces GigabitEthernet 5/4 transceiver
Transceiver Type      : 1000BASE-SX-SFP
Connector Type       : LC
Wavelength(nm)      : 850
Transfer Distance    :
    50/125 um OM2 fiber
        -- 550m
    62.5/125 um OM1 fiber
        -- 270m
Digital Diagnostic Monitoring : YES
Vendor Serial Number      : 101680093602489
```

The following example displays the alarm message of the transceiver of interface GigabitEthernet 5/4.

```
Ruijie#show interfaces GigabitEthernet 5/4 transceiver alarm
gigabitEthernet 5/4 transceiver current alarm information:
RX loss of signal
```

The following example displays the diagnostic parameters of the transceiver of interface GigabitEthernet 5/4.

```
Ruijie#show interfaces GigabitEthernet 5/4 transceiver diagnosis
Current diagnostic parameters[AP:Average Power]:
Temp (Celsius)   Voltage (V)      Bias (mA)          RX power (dBm)      TX
power (dBm)
38 (OK)          3.20 (OK)          0.04 (OK)          -40.00 (alarm) [AP]
-40.00 (alarm)
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.26 show interfaces usage

Use this command to display bandwidth usage of the interface.

show interfaces [*interface-type interface-number*] **usage** [*up* | *down*]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	(Optional) The interface type and ID.
	<i>up</i>	(Optional) Displays the port up statistics.
	<i>down</i>	(Optional) Displays the port down statistics.

Defaults N/A


Command Mode Any CLI mode

Usage Guide If you do not specify an interface, the bandwidth usage of all interfaces is displayed. Bandwidth refers to the actual link bandwidth rather than the *bandwidth* parameter configured on the interface.

Configuration Examples The following example displays bandwidth usage of interface GigabitEthernet 0/1.

```

Interface           Bandwidth   Average Usage   Output Usage
Input Usage
-----
GigabitEthernet 0/0   1000 Mbit    0.002822759%   0.001183280%
0.004462237%
```

 Bandwidth refers to the interface link bandwidth, the maximum speed of link. Average Usage refers to the current usage.

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.27 shutdown

Use this command to disable an interface. Use the **no** form of this command to enable a disabled port.

shutdown


no shutdown

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the administrative status of an interface is Up.

Command Mode Interface configuration mode

Usage Guide Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

 If you use the script to run no shutdown frequently and rapidly, the system may prompt the interface status reversal.

Configuration Examples The following example disables an interface.

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# shutdown
```

The following example enables an interface.

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# no shutdown
```

Related Commands	Command	Description
	clear interface	Resets the hardware.
	show interfaces	Displays the interface information.

Platform Description N/A

1.28 snmp trap link-status

Use this command to send LinkTrap on a port. Use the **no** form of this command to disable this function.

snmp trap link-status
no snmp trap link-status

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default

Command Mode Interface configuration mode.

Usage Guide For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

Configuration Examples The following example disables the interface from sending LinkTrap on the interface.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

The following example enables the interface to forward Link trap.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# snmp trap link-status
```

Related Commands

Command	Description
snmp trap link-status	Enables the interface to send LinkTrap on the interface.
no snmp trap link-status	Disables the interface from sending LinkTrap on the interface.

Platform Description N/A

1.29 snmp-server if-index persist

Use this command to set the interface index persistence. The interface index remains the same after the device is restarted.

snmp-server if-index persist

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this command is configured, all interface indexes are saved in the configuration file. After the

device is restarted, interface indexes remain the same as before.

Configuration The following example enables the interface index persistence.

Examples

```
Ruijie(config)# snmp-server if-index persist
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

1.30 speed

Use this command to configure the speed on the port. Use the **no** form of this command to restore the default setting.

speed [10 | 100 | 1000 | auto]

**Parameter
Description**

Parameter	Description
10	The transmission rate of the interface is 10Mbps.
100	The transmission rate of the interface is 100Mbps.
1000	The transmission rate of the interface is 1000Mbps.
auto	Self-adaptive

Defaults The default is **auto**.

**Command
Mode** Interface configuration mode.

Usage Guide If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M or 100M.

Configuration The following example sets the speed on interface gigabitethernet 1/1 to 100Mbps.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# speed 100
```

**Related
Commands**

Command	Description
show interfaces	Displays the interface information.

Platform N/A

Description

1.31 switchport

Use this command to configure a Layer 3 interface. Use the **no** form of this command to restore the default setting.

switchport

no switchport

Parameter Description

Parameter	Description
N/A	N/A

Defaults All the interfaces are in Layer 2 mode by default.

Command Interface configuration mode.

Mode

Usage Guide This command is valid only for physical interfaces. The **switchport** command is used to disable the interface and re-enable it. In this status, the device will send the information to indicate the connect status. If the interface is changed to Layer 3 mode from Layer 2, all the attributes in Layer 2 mode will be cleared.

Configuration The following example configures a Layer 3 interface.

Examples

```
Ruijie(config-if) # switchport
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform N/A

Description

1.32 switchport access

Use this command to configure an interface as a statics access port and add it to a VLAN. Use the **no** form of this command to restore the default setting.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter

Parameter	Description
-----------	-------------

Description		
	<i>vlan-id</i>	The VLAN ID at which the port to be added.
Defaults	By default, the switch port is an access port and the VLAN is VLAN 1.	
Command Mode	Interface configuration mode.	
Usage Guide	Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN. If the port is a trunk port, the operation does not take effect.	
Configuration Examples	The following example configures interface gigabitethernet 1/1 as a statistic access port and adds it to VLAN 2.	
	<pre>Ruijie(config)# interface gigabitethernet 1/1 Ruijie(config-if)# switchport access vlan 2</pre>	
Related Commands	Command	Description
	switchport mode	Configures the interface as Layer 2 mode (switch port mode).
	switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunkport.
Platform Description	N/A	

1.33 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the **no** form of this command to restore the default setting.

switchport mode { access | trunk }

no switchport mode

Parameter Description	Parameter	Description
	access	Configures the switch port as an access port.
	trunk	Configures the switch port as a trunk port.

Defaults The default is **access**.

Command Interface configuration mode.
Mode

Usage Guide If a switch port mode is access port, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN.
 A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.

Configuration The following example specifies a L2 interface (switch port) mode.

Examples

```
Ruijie(config-if) # switchport mode trunk
```

Related Commands	Command	Description
	switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
	switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunk port.

Platform N/A
Description

1.34 switchport protected

Use this command to configure the interface as the protected port. Use the **no** form of this command to restore the default setting.

switchport protected
no switchport protected

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Interface configuration mode.
Mode

Usage Guide The ports that are set as the protected ports cannot switch on L2, but can route on L3. A protected port can communicate with an unprotected port. Use the **show interfaces** command to display configuration.

Configuration The following example configures interface `gigabitethernet 1/1` as a protected port.

Examples

```
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)# switchport protected
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform N/A

Description

1.35 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of this command to restore the default setting.

switchport trunk { allowed vlan { all | [add | remove | except] *vlan-list* } | native vlan *vlan-id* }
no switchport trunk { allowed vlan | native vlan }

Parameter Description

Parameter	Description
allowed vlan <i>vlan-list</i>	Configures the list of VLANs allowed on the trunk port. <i>vlan-list</i> can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma (,), for example, 1 to 10, 20 to 25, 30, 33. all means that the allowed VLAN list contains all the supported VLANs; add means to add the specified VLAN list to the allowed VLAN list; remove means to remove the specified VLAN list from the allowed VLAN list; except means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
native vlan <i>vlan-id</i>	Configures the native VLAN.

Defaults The allowed VLAN list is all, the Native VLAN is VLAN1.

Command Mode Interface configuration mode.

Usage Guide Native VLAN:

A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface

(that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged.

Allowed-VLAN List:

By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk by configuring allowed VLAN lists on a trunk. Use `show interfaces switchport` to display configuration.

Configuration The following example removes port 1/15 from VLAN 2.

Examples

```
Ruijie(config)# interface fastethernet 1/15
Ruijie(config-if)# switchport trunk allowed vlan remove 2
Ruijie(config-if)# end
Ruijie# show interfaces fastethernet1/15 switchport
Switchport is enabled
Mode is trunk port
Access vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is
1,3-4094
```

**Related
Commands**

Command	Description
show interfaces	Displays the interface information.
switchport access	Configures an interface as a statics access port and assigns it to a VLAN.

**Platform
Description** N/A

2 MAC Address Commands

2.1 clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

```
clear mac-address-table dynamic [ address mac-addr [ interface interface-id ] [ vlan vlan-id ] |
{ [ interface interface-id ] [ vlan vlan-id ] }
```

Parameter	Parameter	Description
Description	dynamic	Clears all the dynamic MAC addresses.
	address <i>mac-addr</i>	Clears the specified dynamic MAC address.
	interface <i>interface-id</i>	Clears all the dynamic MAC addresses of the specified interface.
	vlan <i>vlan-id</i>	Clears all the dynamic MAC addresses of the specified VLAN, in the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use the **show mac-address-table dynamic** command to display all the dynamic MAC addresses.

Configuration Examples The following command clears all the dynamic MAC addresses.

```
Ruijie# clear mac-address-table dynamic
```

Related Commands	Command	Description
	show mac-address-table dynamic	Displays dynamic MAC address.

Platform N/A

Description

2.2 mac-address-learning

Use this command to enable the port address learning. Use the **no** or **default** form of this command to restore the default setting.

mac-address-learning

no mac-address-learning

default mac-address-learning

Parameter	Parameter	Description
-----------	-----------	-------------

Description	N/A					
Defaults	The address learning function is enabled.					
Command Mode	Interface configuration mode.					
Usage Guide	MAC address learning cannot be disabled on the port where the security function is enabled. The security function cannot be configured on the port where address learning is disabled.					
Configuration Examples	The following example disables the port address learning function.					
Examples	<pre>Ruijie(config-if)# no mac-address-learning</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

2.3 mac-address-learning (global)

Use this command to enable MAC address learning globally. Use the **no** or **default** form of this command to restore the default setting.

mac-address-learning enable

Use this command to disable MAC address learning globally.

mac-address-learning disable

Use this command to restore MAC address learning globally.

default mac-address-learning

Parameter Description	Parameter	Description
	enable	Enables MAC address learning globally.
	disable	Disables MAC address learning globally.

Defaults	The mac-address-learning enable command is enabled by default.
Command Mode	Global configuration mode
Usage Guide	When this function is enabled, the MAC address is learned in global configuration mode the same as learned in interface configuration mode.
Configuration Examples	The following example disables MAC address learning globally.
Examples	<pre>Ruijie(config)# mac-address-learning disable</pre>

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

2.4 mac-address-table aging-time

Use this command to specify the aging time of the dynamic MAC address. Use the **no** or **default** form of the command to restore the default setting.

mac-address-table aging-time *seconds*

no mac-address-table aging-time

default mac-address-table aging-time

Parameter	Parameter	Description
Description	<i>seconds</i>	Aging time of the dynamic MAC address (in seconds). The time range depends on the switch.

Defaults The default is 300.

Command Global configuration mode.
Mode

Usage Guide Use **show mac-address-table aging-time** to display configuration.

Configuration The following example sets the aging time of the dynamic MAC address to 500 seconds.

Examples

```
Ruijie(config)# mac-address-table aging-time 500
```

Related	Command	Description
Commands	show mac-address-table aging-time	Displays the aging time of the dynamic MAC address.
	show mac-address-table dynamic	Displays dynamic MAC address.

Platform N/A
Description

2.5 mac-address-table filtering

Use this command to configure the filtering MAC address. Use the **no** or **default** form of the command to restore the default setting.

mac-address-table filtering *mac-address* **vlan** *vlan-id*

no mac-address-table filtering *mac-address* **vlan** *vlan-id*

default mac-address-table filtering *mac-address* **vlan** *vlan-id*

Parameter	Parameter	Description
Description	<i>mac-address</i>	Filtering Address
	<i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.

Defaults No filtering address is configured by default.

Command Global configuration mode.

Mode

Usage Guide The filtering MAC address shall not be a multicast address.

Configuration The following example configures the filtering MAC address for VLAN 1.

Examples

```
Ruijie(config)#mac-address-table filtering 0000.0202.0303 vlan 3
```

Related	Command	Description
Commands	clear mac-address-table filtering	Clears the filtering MAC address.

Platform N/A

Description

2.6 mac-address-table flapping-logging

Use this command to enable MAC-flapping logging Use the **no** or **default** form of this command to restore the default setting.

mac-address-table flapping-logging

no/default mac-address-table flapping-logging

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide Use this command to enable logging for MAC-flapping among different ports within a VLAN.

Configuration The following example enables MAC-flapping logging.

Examples

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table flapping-logging
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.7 mac-address-table notification

Use this command to enable the MAC address notification function. Use The **no** or **default** form of the command to restore the default setting.

mac-address-table notification [**interval** *value* | **history-size** *value*]

no mac-address-table notification [**interval** | **history-size**]

default mac-address-table notification [**interval** | **history-size**]

Parameter Description	Parameter	Description
	interval <i>value</i>	Sets the interval of sending the MAC address trap message, 1 second by default.
	history-size <i>value</i>	Sets the maximum number of the entries in the MAC address notification table, 50 entries by default.

Defaults By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.

Command Mode Global configuration mode.

Usage Guide The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the **snmp-server enable traps mac-notification** command to enable or disable the switch to send the MAC address trap message.

Configuration Examples The following example enables the MAC address notification function.

```
Ruijie(config)# mac-address-table notification
Ruijie(config)# mac-address-table notification interval 40
Ruijie(config)# mac-address-table notification history-size 100
```

Related Commands	Command	Description
	snmp-server enable traps	Sets the method of handling the MAC address trap message..
	show mac-address-table notification	Displays the MAC address notification configuration and the MAC address trap notification table.
	snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.

Platform N/A

Description

2.8 mac-address-table static

Use this command to configure a static MAC address. Use the **no** or **default** form of the command to restore the default setting.

mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

default mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Parameter	Parameter	Description
Description	<i>mac-addr</i>	Destination MAC address of the specified entry
	<i>vlan-id</i>	VLAN ID of the specified entry, in the range from 1 to 4094.
	<i>interface-id</i>	Interface (physical interface or aggregate port) that packets are forwarded to

Defaults No static MAC address is configured by default.

Command Global configuration mode.

Mode

Usage Guide A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use `show mac-address-table static` to display the static MAC address.

Configuration N/A

Examples

Related	Command	Description
Commands	show mac-address-table static	Displays the static MAC address.

Platform N/A

Description

2.9 max-dynamic-mac-count

Use this command to set the maximum number of MAC address learned dynamically on the VLAN or interface. Use the **no** or **default** form of this command to restore the default setting.

max-dynamic-mac-count *num*

no max-dynamic-mac-count

default max-dynamic-mac-count

Parameter	Parameter	Description
Description	<i>num</i>	Sets the maximum number of MAC addresses.

Defaults The maximum number is not set by default.

Command VLAN configuration mode / Interface configuration mode

Mode

Usage Guide This command is used to set the maximum number of MAC addresses learned dynamically on the VLAN or interface.

If the number of MAC addresses dynamically learned on the VLAN or interface reaches the upper limit, MAC address learning is disabled on the VLAN or interface.

If the number of MAC addresses reaches the upper limit when this command is configured, the surplus MAC addresses are not cleared. Instead, they remain and then age. MAC address learning is disabled on the VLAN or interface.

Use the **show mac-address-table max-dynamic-mac-count** command to display the maximum number of MAC addresses learned dynamically on the VLAN or interface.

Configuration The following example sets the maximum number of MAC addresses dynamically learned on VLAN

Examples

1.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 1
Ruijie(config-vlan)#max-dynamic-mac-count 160
```

The following example sets the maximum number of MAC addresses dynamically learned on interface GigabitEthernet 0/1.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count 160
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

2.10 max-dynamic-mac-count exceed-action

Use this command to set the action if the dynamic MAC address learned on the VLAN or interface exceeds the limit. Run the no form of this command to restore the default setting.

max-dynamic-mac-count exceed-action forward | discard

no max-dynamic-mac-count exceed-action *forward | discard*

Parameter	Parameter	Description
Description	<i>forward</i>	Forwards the packets if the dynamic MAC address learned on the VLAN or interface exceeds the limit.
	<i>discard</i>	Discards the packets if the dynamic MAC address learned on the VLAN or interface exceeds the limit.

Command Mode VLAN configuration mode / Interface configuration mode

Usage Guide This command is used to set the action if the dynamic MAC address learned on the VLAN or interface exceeds the limit.

Configuration Examples The following example sets the maximum number of MAC addresses dynamically learned on VLAN 1.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#vlan 1
Ruijie(config-vlan)#max-dynamic-mac-count 160
Ruijie(config-vlan)#max-dynamic-mac-count exceed-action discard
```

The following example sets the maximum number of MAC addresses dynamically learned on interface GigabitEthernet 0/1.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count 100
Ruijie(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count exceed-action
discard
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.11 show mac-address-learning

Use this command to display the MAC address learning.

show mac-address-learning

Parameter	Parameter	Description
-----------	-----------	-------------

Description	N/A	N/A				
Defaults	N/A					
Command Mode	Privileged EXEC mode.					
Usage Guide	N/A					
Configuration	The following example displays the MAC address learning.					
Examples	<pre>Ruijie# show mac-address-learning GigabitEthernet 0/0 learning ability: disable GigabitEthernet 0/1 learning ability: enable GigabitEthernet 0/2 learning ability: enable GigabitEthernet 0/3 learning ability: enable</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

2.12 show mac-address-table

Use this command to display all types of MAC addresses (including dynamic address, static address and filter address).

show mac-address-table [**address** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter Description	Parameter	Description
	address <i>mac-addr</i>	The MAC address.
	interface <i>interface-id</i>	The Interface ID.
	vlan <i>vlan-id</i>	The VLAN ID, in the range from 1 to 4094.
Defaults	N/A	
Command Mode	All modes	
Usage Guide	N/A	

Configuration The following example displays the MAC address.

Examples

```
Ruijie# show mac-address-table address 00d0.f800.1001
Vlan      MAC Address      Type      Interface
```

```

-----
1          00d0.f800.1001      STATIC GigabitEthernet 1/1
Ruijie# show mac-address-table
Vlan      MAC Address      Type      Interface
-----
1          00d0.f800.1001      STATIC GigabitEthernet 1/1
1          00d0.f800.1002      DYNAMIC GigabitEthernet 1/1
1          00d0.f800.1003      OTHER   GigabitEthernet 1/1
1          00d0.f800.1004      FILTER
    
```

Field	Description
Vlan	The interface address.
MAC Address	The MAC address.
Type	The MAC address type.
Interface	The interface corresponding to the MAC address.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.13 show mac-address-table aging-time

Use this command to display the aging time of the dynamic MAC address.

show mac-address-table aging-time

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the aging time of the dynamic MAC address.

```

Ruijie# show mac-address-table aging-time
Aging time : 300
    
```

Related Commands	Command	Description
	mac-address-table aging-time	Sets the aging time of the dynamic MAC address.

Platform N/A
Description

2.14 show mac-address-table count

Use this command to display the number of address entries in the address table.

show mac-address-table count [**interface** *interface-id*] **vlan** *vlan-id*]

Parameter	Parameter	Description
Description	interface <i>interface-id</i>	Interface ID
	vlan <i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide The **show mac-address-table count** command is used to display the number of entries based on the type of MAC address entry.

The **show mac-address-table count interface** command is used to display the number of entries based on the interface associated with the MAC address entry.

The **show mac-address-table count vlan** command is used to display the number of entries based on the VLAN of MAC address entries.

Configuration The following example displays the number of MAC address entries.

Examples Ruijie# show mac-address-table count

```
Dynamic Address Count : 51
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses : 51
Total Mac Address Space Available: 8139
```

The following example displays the number of MAC address in VLAN 1.

```
Ruijie# show mac-address-table count vlan 1
Dynamic Address Count : 7
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses : 7
```

The following example displays the number of MAC addresses on interface g0/1.

```
Ruijie# show mac-address-table interface g0/1
Dynamic Address Count : 10
Static Address Count : 0
Filter Address Count : 0
```

```
Total Mac Addresses : 10
```

Related Commands	Command	Description
	show mac-address-table static	Displays the static address.
	show mac-address-table filtering	Displays the filtering address.
	show mac-address-table dynamic	Displays the dynamic address.
	show mac-address-table address	Displays all the address information of the specified address.
	show mac-address-table interface	Displays all the address information of the specified interface.
	show mac-address-table vlan	Displays all the address information of the specified vlan.

Platform N/A

Description

2.15 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

show mac-address-table dynamic [**address** *mac-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter Description	Parameter	Description
	<i>mac-addr</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN of the entry, in the range from 1 to 4094.
	<i>interface-id</i>	Interface that the packet is forwarded to. It may be a physical port or an aggregate port

Defaults All the MAC addresses are displayed by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the dynamic MAC address.

```
Ruijie# show mac-address-table dynamic
Vlan  MAC Address      Type      Interface
-----
1      0000.0000.0001      DYNAMIC  gigabitethernet 1/1
1      0001.960c.a740      DYNAMIC  gigabitethernet 1/1
1      0007.95c7.dff9      DYNAMIC  gigabitethernet 1/1
1      0007.95cf.eee0      DYNAMIC  gigabitethernet 1/1
1      0007.95cf.f41f      DYNAMIC  gigabitethernet 1/1
1      0009.b715.d400      DYNAMIC  gigabitethernet 1/1
```

```
1 0050.bade.63c4 DYNAMIC gigabitethernet 1/1
```

Related Commands	Command	Description
	clear mac-address-table dynamic	Clears the dynamic MAC address.

Platform N/A

Description

2.16 show mac-address-table filtering

Use this command to display the filtering MAC address.

show mac-address-table filtering [*ddr mac-addr*] [*vlan vlan-id*]

Parameter	Parameter	Description
Description	<i>mac-addr</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN ID of the entry, in the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the filtering MAC address.

```
Ruijie# show mac-address-table filtering
Vlan  MAC Address  Type  Interface
-----
1     0000.2222.2222  FILTER Not available
```

Related Commands	Command	Description
	mac-address-table filtering	Configures the filtering MAC address.

Platform N/A

Description

2.17 show mac-address-table interface

Use this command to display all the MAC addresses on the specified interface including static and dynamic MAC address

show mac-address-table interface [*interface-id*] [*vlan vlan-id*]

Parameter	Parameter	Description
-----------	-----------	-------------

Description	<i>interface-id</i>	Displays the MAC address information of the specified Interface (physical interface or aggregate port).
	<i>vlan-id</i>	VLAN ID of the entry, in the range from 1 to 4094..

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays all the MAC addresses on interface gigabitethernet 1/1.

Examples

```
Ruijie# show mac-address-table interface
gigabitethernet 1/1
Vlan  MAC Address  Type  Interface
-----
1     00d0.f800.1001  STATIC  gigabitethernet 1/1
1     00d0.f800.1002  STATIC  gigabitethernet 1/1
1     00d0.f800.1003  STATIC  gigabitethernet 1/1
1     00d0.f800.1004  STATIC  gigabitethernet 1/1
```

Related Commands	Command	Description
		show mac-address-table static
	show mac-address-table filtering	Displays the filtering MAC address.
	show mac-address-table dynamic	Displays the dynamic MAC address.
	show mac-address-table address	Displays all types of MAC addresses.
	show mac-address-table vlan	Displays all types of MAC addresses of the specified VLAN.
	show mac-address-table count	Displays the address counts in the MAC address table.

Platform N/A

Description

2.18 show mac-address-table max-dynamic-mac-count

Use this command to display the maximum number of dynamic MAC addresses learned on the VLAN or interface.

show mac-address-table max-dynamic-mac-count { vlan [*vlan-id*] | interface [*interface-id*] }

Parameter Description	Parameter	Description
		vlan
	<i>vlan-id</i>	Displays the dynamic MAC address learned on the specified

	VLAN.
interface	Displays the dynamic MAC address learned on all interfaces which are configured with the maximum number of dynamic MAC address learning.
<i>interface-id</i>	Displays the dynamic MAC address learned on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the MAC address learned on all VLANs which are configured with the maximum number of dynamic MAC addresses.

```
Ruijie#show mac-address-table max-dynamic-mac-count vlan
Vlan Limit  MAC count Learning
-----
1  160      6      YES
```

The following example displays the MAC address learned dynamically on the specified VLAN.

```
Ruijie#show mac-address-table max-dynamic-mac-count vlan 1
Vlan Limit  MAC count Learning
-----
1  160      6      YES
```

Field	Description
Vlan	The VLAN ID.
Limit	The maximum number of MAC addresses.
MAC count	The number of MAC address learned dynamically on the VLAN.
Learning	Whether MAC address learning is disabled on the VLAN.

The following example displays the MAC address learned on all interfaces which are configured with the maximum number of the dynamic MAC address.

```
Ruijie#show mac-address-table max-dynamic-mac-count interface
Interface          Limit  MAC count Learning
-----
GigabitEthernet 0/1  160   6      YES
```

The following example displays the MAC address learned dynamically on the specified interface.

```
Ruijie#show mac-address-table max-dynamic-mac-count interface
GigabitEthernet 0/1
Interface          Limit  MAC count Learning
-----
GigabitEthernet 0/1  160   6      YES
```

Field	Description
Interface	The Interface ID
Limit	The maximum number of MAC addresses.
MAC count	The number of MAC address learned dynamically on the interface.
Learning	Whether MAC address learning is disabled on the interface

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.19 show mac-address-table notification

Use this command to display the MAC address notification configuration and the MAC address notification table.

show mac-address-table notification [interface [*interface-id*] | history]

Parameter Description	Parameter	Description
	interface	Displays the MAC address notification configuration on all interfaces.
	interface <i>interface-id</i>	Displays the MAC address notification configuration on a specific interface.
	history	Displays the MAC address notification history.

Defaults The MAC address notification configuration is displayed by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the MAC address notification configuration and the MAC address notification table.

```
Ruijie# show mac-address-table notification interface
Interface      MAC Added Trap  MAC Removed Trap
-----
GigabitEthernet1/14  Disabled      Disabled
Ruijie# show mac-address-table notification
MAC Notification Feature: Disabled
Interval between Notification Traps: 1 secs
```

```

Maximum Number of entries configured in History Table:1
Current History Table Length: 0
Ruijie# show mac-address-table notification history
History Index: 0
MAC Changed Message:
Operation:ADD Vlan: 1 MAC Addr: 00f8.d012.3456 GigabitEthernet 3/1

```

Related Commands	Command	Description
	mac-address-table notification	Enables MAC address notification.
	snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.

Platform N/A

Description

2.20 show mac-address-table static

Use this command to display the static MAC address.

show mac-address-table static [**addr** *mac-addr* *r*] [**interface** *interface-Id*] [**vlan** *vlan-id*]

Parameter Description	Parameter	Description
	<i>mac-addr</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN ID of the entry, within the range from 1 to 4094.
	<i>interface-id</i>	Interface of the entry physical interface or aggregate port

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays the static MAC addresses

Examples

```

Ruijie# show mac-address-table static
Vlan   MAC Address      Type   Interface
-----
1 00d0.f800.1001  STATIC gigabitethernet 1/1
1 00d0.f800.1002  STATIC gigabitethernet 1/1
1 00d0.f800.1003  STATIC gigabitethernet 1/1

```

Related Commands	Command	Description
	mac-address-table static	Configures the static MAC address.

Platform N/A

Description

2.21 show mac-address-table vlan

Use this command to display all addresses of the specified VLAN.

show mac-address-table vlan [*vlan-id*]

Parameter	Parameter	Description
Description	<i>vlan-id</i>	VLAN ID of the entry, within the range from 1 to 4094.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays all addresses of the specified VLAN.

Examples

```
Ruijie# show mac-address-table vlan 1
Vlan  MAC Address      Type      Interface
-----
1      00d0.f800.1001      STATIC    gigabitethernet 1/1
1      00d0.f800.1002      STATIC    gigabitethernet 1/1
1      00d0.f800.1003      STATIC    gigabitethernet 1/1
```

Related Commands	Command	Description
	show mac-address-table static	Displays static addresses.
	show mac-address-table filtering	Displays filtered addresses.
	show mac-address-table dynamic	Displays dynamic addresses.
	show mac-address-table address	Displays all address information about the specified address.
	show mac-address-table interface	Displays all address information about the specified interface.
	show mac-address-table count	Displays the number of addresses in the address table.

Platform N/A

Description

2.22 snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. Use The **no** or **default** form of the command to restore the default setting.

```
snmp trap mac-notification { added | removed }
no snmp trap mac-notification { added | removed }
default snmp trap mac-notification { added | removed }
```

Parameter	Parameter	Description
Description	<i>added</i>	Notifies when a MAC address is added.
	<i>removed</i>	Notifies when a MAC address is removed

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide Use **show mac-address-table notification interface** to display configuration.

Configuration Examples The following example enables the MAC address trap notification on interface gigabitethernet 1/1.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# snmp trap mac-notification added
```

Related Commands	Command	Description
	mac-address-table notification	Enables MAC address notification.
	show mac-address-table notification	Displays the MAC address notification configuration and the MAC address notification table.

Platform Description N/A

3 Aggregate Port Commands

3.1 aggregate bfd-detect

Use this command to enable BFD on the AP port. Use the **no** form of this command to restore the default setting.

aggregate bfd-detect { **ipv4** } *src_ip dst_ip*

no aggregate bfd-detect { **ipv4** }

Parameter Description	Parameter	Description
	ipv4	Enables IPv4 BFD when the AP port is configured with an IPv4 address.
	<i>src_ip</i>	Specifies source IP address, namely, the IP address configured on the AP port.
	<i>dst_ip</i>	Specifies destination IP address, namely, the IP address configured on the peer AP port.

Defaults This function is disabled by default.

Command Mode AP interface configuration mode

Usage Guide If you want to enable BFD on the AP port, you should see corresponding configuration guide for BFD parameter settings.

Different products vary in support for IPv4/IPv6 BFD on AP port.

If an AP port supports both IPv4 and IPv6 BFD, it is allowed to enable both IPv4 and IPv6 BFD at the same time.

If an AP port is enabled with BFD, its member ports in forwarding state create BFD session automatically.

Configuration Examples The following example enables BFD on the AP port.

```
Switch(config)# interface aggregateport 3
Switch(config-if-Aggregateport 3)# ip address 1.0.0.1
Switch(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
Switch(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.2 aggregateport capacity mode

Use this command to configure the AP capacity mode. Use the **no** form of this command to restore the default setting, Use the **no** form of this command to restore the default setting,

aggregateport capacity mode *capacity-mode*

no aggregateport capacity mode

Parameter	Parameter	Description
Description	<i>capacity-mode</i>	Configures the capacity mode.

Defaults The default *capacity-mode* varies with the device.

Command Mode Global configuration mode

Usage Guide The system provides several capacity modes for devices that support capacity mode configuration. To restore the default settings, run **no aggregateport capacity mode** in global configuration mode.

Configuration Examples The following example configures the the capacity mode.

Ruijie# configure terminal

Ruijie(config)# aggregateport capacity mode 256*8

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.3 aggregateport load-balance

Use this command to configure a global load-balance algorithm for aggregate ports or a load-balance algorithm for an aggregate port . Use the **no** form of this command to return the default setting.

aggregateport load-balance { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst ip** | **src-dst-ip-l4port** | **enhanced profile profile-name** }

no aggregateport load-balance

Parameter	Parameter	Description
Description	dst-mac	Load balance based on the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.

src-mac	Load balance based on the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-ip	Load balance based on the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
dst-ip	Load balance based on the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Load balance based on the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-mac	Load balance based on the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.
src-dst-ip-l4port	Load balance based on the source IP address, destination IP address, L4 source port number and L4 destination port number.
enhanced profile	Load balance based on the packet type

Defaults The default load balance mode is **src-dst-mac** for the L2 AP port and **src-dst-ip** for the L3 AP port .

Command Mode Global configuration mode/Interface configuration mode

Usage Guide You can run `aggregateport load-balance` in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run `no aggregateport load-balance` in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect.

Configuration Examples The following example configures a load-balance algorithm globally based on the destination MAC address.

```
Ruijie(config)# aggregateport load-balance dst-mac
```

Related Commands	Command	Description
	show aggregateport load-balance	Displays aggregate port configuration.

Platform N/A

Description

3.4 aggregateport member linktrap

Use this command to send LinkTrap to aggregate port members. Use the **no** form of this command to restore the default setting.

aggregateport member linktrap

no aggregateport member linktrap

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide This function cannot be enabled by running the **snmp trap link-status** command in interface configuration mode.

Configuration The following example enables the LinkTrap function on the aggregate port members.

Examples

```
Ruijie# configure terminal
Ruijie(config)# aggregateport member linktrap
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.5 fcoe field

Use this command to set the load balance mode of FCOE packets for the specified template. Use the **no** form of this command to restore the default setting.

fcoe field [vlan] [src-port] [dst-port] [src-id] [dst-id] [rx-id] [ox-id] [fabric-id]

no fcoe field

Parameter	Parameter	Description
Description	vlan	Load balance based on VLAN ID of FCOE packets.
	src-port	Load balance based on the source port number of FCOE packets.
	dst-port	Load balance based on the destination port number of FCOE packets.
	src-id	Load balance based on the source ID of FCOE packets.

dst-id	Load balance based on the destination ID of FCOE packets.
rx-id	Load balance based on the Responder Exchange ID of FCOE packets.
ox-id	Load balance based on the Originator Exchange ID of FCOE packets.
fabric-id	Load balance based on the Fabric ID of the FC network of FCOE packets..

Defaults The default load balance mode is **src-id**, **dst-id** and **ox-id**.

Command Mode Enhanced template configuration mode

Usage Guide The enhance template should be configured first.

Configuration Examples The following example sets the load balance mode for FCOE packets to **src-id** and **src-port**.

```
Ruijie(config)# load-balance-profile apl
Ruijie(config-load-balance-profile)# fcoe field src-id src-port
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.6 interfaces aggregateport

Use this command to create the aggregate port or enter interface configuration mode of the aggregate port. Use the **no** form of this command to restore the default setting.

interfaces aggregateport *ap-number*

no interfaces aggregateport *ap-number*

Parameter Description	Parameter	Description
	<i>ap-number</i>	Aggregate port number.

Defaults The aggregate port is not created by default.

Command Mode Global configuration mode

Usage Guide If the aggregate port is created, this command is used to enter the interface configuration mode. Otherwise, this command is used to create the aggregate port and then enter its interface configuration mode.

Configuration Examples The following example creates AP 5 and enters its interface configuration mode.

```
Ruijie# configure terminal
```

```
Ruijie(config)# interfaces aggregateport 5
Ruijie(config-if-Aggregateport 5)# end
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.7 ipv4 field

Use this command to configure the IPv4 load balance mode for a specified profile. Use the **no** form of this command to restore the default setting.

ipv4 field [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**vlan**] [**src-port**]
no ipv4 field

Parameter Description	Parameter	Description
	src-ip	Load balance based on the source IP address of the IPv4 packet.
	dst-ip	Load balance based on the destination IP address of the IPv4 packet.
	protocol	Load balance based on the protocol type of the IPv4 packet.
	l4-src-port	Load balance based on the L4 source port number of the IPv4 packet.
	l4-dst-port	Load balance based on the L4 destination port number of the IPv4 packet.
	vlan	Load balance based on the VLAN ID of the IPv4 packet.
	src-port	Load balance based on the source port number of the IPv4 packet.

Defaults The default load balance mode is **src-ip** and **dst-ip**.

Command Mode Load balance profile configuration mode

Usage Guide You need to configure the load balance profile first.

Configuration Examples The following example sets the IPv4 load balance mode for profile apl to **src-ip**.

```
Ruijie# configure terminal
Ruijie(config)# load-balance-profile apl
Ruijie(config-load-balance-profile)# ipv4 field src-ip
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.8 ipv6 field

Use this command to configure the IPv6 load balance mode for a specified profile. Use the **no** form of this command to restore the default setting.

ipv6 field [**src-ip**] [**dst-ip**] [**protocol**] [**I4-src-port**] [**I4-dst-port**] [**vlan**] [**src-port**]
no ipv6 field

Parameter	Parameter	Description
Description	src-ip	Load balance based on the source IP addresses of the IPv6 packets.
	dst-ip	Load balance based on the destination IP addresses of the IPv6 packets.
	protocol	Load balance based on the protocol types of the IPv6 packets.
	I4-src-port	Load balance based on the L4 source port numbers of the IPv6 packets.
	I4-dst-port	Load balance based on the L4 destination port numbers of the IPv6 packets.
	vlan	Load balance based on the VLAN ID of the IPv6 packets.
	src-port	Load balance based on the source port numbers of the IPv6 packets.

Defaults The default load balance mode is **src-ip** and **dst-ip**.

Command Mode Load balance profile configuration mode

Usage Guide You need to configure the load balance profile first.

Configuration Examples The following example sets the load balance mode of IPv6 packets to **src-ip**.

```
Ruijie(config)# load-balance-profile apl
Ruijie(config-load-balance-profile)# ipv6 field src-ip
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.9 I2 field

Use this command to configure the load balance mode of L2 packets for a specified profile. Use the **no** form of this command to restore the default setting.

I2 field [**src-mac**] [**dst-mac**] [**I2-protocol**] [**vlan**] [**src-port**]
no I2 field

Parameter	Parameter	Description
-----------	-----------	-------------

Description	src-mac	Load balance based on the source MAC address of the L2 packet.
	dst-mac	Load balance based on the destination MAC address of the L2 packets.
	l2-protocol	Load balance based on the L2 protocol type of the L2 packet.
	vlan	Load balance based on the VLAN ID of the L2 packet.
	src-port	Load balance based on the source port number of the L2 packet.

Defaults The default load balance mode is **src-mac**, **dst-mac**, and **vlan**.

Command Mode Load balance profile configuration mode

Usage Guide You need to configure the load balance profile first.

Configuration Examples The following example sets the load balance mode of L2 packets to **src-mac** and **src-prot**.

```
Ruijie(config)# load-balance-profile apl
Ruijie(config-load-balance-profile)# l2 field src-mac src-port
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.10 lacp port-priority

Use this command to set the priority of the LACP AP member port. Use the **no** form of this command to restore the default setting.

lacp port-priority *port-priority*
no lacp port-priority

Parameter Description	Parameter	Description
	<i>port-priority</i>	The LACP port priority, in the range from 0 to 65535.

Defaults The default is 32768.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration This example sets the LACP port priority of interface Gi0/1 to 4096.

Examples

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lacp port-priority 4096
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.11 lacp short-timeout

Use this command to configure the short-timeout mode for the LACP AP member port. Use the no form of this command to restore the default setting.

lacp short-timeout

no lacp short-timeout

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults The default is long-timeout mode.

Command Mode Interface configuration mode

Usage Guide In long-timeout mode, the port sends an LACP packet every 30 seconds. If the packet is not received in 90 seconds, the connection times out.
In short-timeout mode, the port sends an LACP packet every 1 second. If the packet is not received in 3 seconds, the connection times out.

Configuration Examples The following example configures the short-timeout mode for the LACP AP member port.

Examples

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lacp short-timeout
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.12 lacp system-priority

Use this command to set the LACP system priority. Use the **no** form of this command to restore the default setting.

lacp system-priority *system-priority*

no lacp system-priority

Parameter Description	Parameter	Description
	<i>system-priority</i>	The LACP system priority, in the range from 0 to 65535.

Defaults The default is 32768.

Command Mode Global configuration mode.

Usage Guide LACP system priority consists of the Layer2 management MAC address and its priority value, where the MAC address is fixed but the priority value is configurable. If two priorities are equal, then the smaller the MAC address is, the higher the priority is. All LACP groups on the switch share the system priority. Changing the system priority may influence the whole aggregation groups on the switch.

Configuration The following example sets the LACP system priority to 4096.

Examples Ruijie(config)# lacp system-priority 4096

Related Commands	Command	Description
	port-group <i>key mode</i> { active passive }	Enables the LACP on the port and specifies the aggregation group ID and operation mode.
	lacp port-priority	Sets the LACP port priority.

Platform N/A

Description

3.13 load-balance-profile

Use this command to rename a load balance enhanced profile and apply the profile. Use the **no** form of this command to restore the load balance configuration without changing the profile name. Use the **default** form of this command to restore the default setting.

load-balance-profile *profile-name*

no load-balance-profile *profile-name*

no load-balance-profile

Parameter	Parameter	Description
Description	<i>profile-name</i>	Specifies the profile name, which contains up to 31 characters.

Defaults The default *profile-name* is default.

Command Global configuration mode.

Mode

Usage Guide By default, the device is configured with an enhanced profile named default. Use the **load-balance-profile default** command to enter the enhanced profile configuration mode. You can change the profile name by using the **load-balance-profile *profile-name*** command.

Configuration The following example creates a load balance profile named **apl**.

Examples

```
Ruijie(config)# load-balance-profile apl
Warning: The profile default has been used, and this command will rename it. Continue? [Y/N]:y
Ruijie(config-load-balance-profile)#
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

3.14 mpls field

Use this command to configure the load balance mode of MPLS packets in a specified load balance enhanced profile. Use the **no** form of this command to restore the default setting.

mpls field [**top-label**] [**2nd-label**] [**src-ip**] [**dst-ip**] [**vlan**] [**src-port**]

no mpls field

Parameter	Parameter	Description
Description	top-label	Load balance based on the destination top labels of the MPLS packets.
	2nd-label	Load balance based on the destination second labels of the MPLS packets.
	src-ip	Load balance based on the source IP addresses of the MPLS packets.
	dst-ip	Load balance based on the destination IP addresses of the MPLS packets.
	vlan	Load balance based on the VLANs of the MPLS packets.
	src-port	Load balance based on the source port numbers of the MPLS packets.

Defaults The default load balance mode is **top-label** and **2nd-label**.

Command Load balance enhanced profile configuration mode.

Mode

Usage Guide Use the **show load-balance-profile** command to display the load balance mode configuration.

Configuration The following example sets the load balance mode of MPLS packets to **top-label** and **src-ip**.

Examples Ruijie(config-load-balance-profile)# mpls field top-label src-ip

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

3.15 port-group

Use this command to assign a physical interface to be a member port of a static aggregate port or an LACP aggregate port. Use the **no** form of this command to restore the default setting.

port-group *port-group-number*

port-group *key-number* **mode** { **active** | **passive** }

no port-group

Parameter	Parameter	Description
Description	<i>port-group-number</i>	Member group ID of an aggregate port, the interface number of the aggregate port.
	<i>key-number</i>	Member group ID of an LACP aggregate port, the interface number of the LACP aggregate port.
	active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
	passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Defaults By default, the physical port does not belong to any aggregate port.

Command Interface configuration mode.

Mode

Usage Guide All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.

Configuration The following example specifies the Ethernet interface 1/3 as a member of the static AP 3.

Examples Ruijie(config)# interface gigabitethernet 1/3

Ruijie(config-if-GigabitEthernet 1/3)# port-group 3

The following example specifies the Ethernet interface 2/3 as a member of the LACP AP4 and set the aggregation mode to active.

Ruijie(config)# interface gigabitethernet 2/3

Ruijie(config-if-GigabitEthernet 2/3)# port-group 4 mode active

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

3.16 show aggregateport

Use this command to display the aggregate port configuration.

show aggregateport { [*aggregate-port-number*] **summary** | **load-balance** }

Parameter	Parameter	Description
Description	<i>aggregate-port-number</i>	Number of the aggregate port.
	load-balance	Displays the load-balance algorithm on the aggregate port.
	summary	Displays the summary of the aggregate port.

Defaults N/A

Command Any mode
Mode

Usage Guide If the aggregate port number is not specified, all the aggregate port information will be displayed.

Configuration The following example displays the aggregate port configuration.

Examples

```
Ruijie# show aggregateport 1 summary
AggregatePort  MaxPorts      SwitchPort Mode    Load balance      Ports
-----
Ag1             8             Enabled  ACCESS  dst-mac            Gi0/2
```

Related	Command	Description
Commands	aggregateport load-balance	Configures a load-balance algorithm of AP.

Platform N/A

Description

3.17 show aggregateport capacity

Use this command to display the AP capacity mode and the AP number.

show aggregateport capacity

Parameter	Parameter	Description
-----------	-----------	-------------

Description	N/A	N/A
--------------------	-----	-----

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays the AP capacity mode and the AP number.

Examples

```
Ruijie# show aggregateport capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 128*16.
Effective Capacity Mode      : 256*8.
Available Capacity          : 128*8.
Total Number: 128, Used: 1, Available: 127.
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.18 show lacp summary

Use this command to display the LACP aggregation information.

show lacp summary [*key*]

Parameter Description	Parameter	Description
	<i>key</i>	

Defaults N/A

Command Mode Any mode.

Usage Guide N/A

Configuration The following example displays the LACP aggregation information.

Examples

```
Ruijie(config)# show lacp summary 3
System Id:32768, 00d0.f8fb.0002
```

```

Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs.
A - Device is in active mode.          P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper  Port  Port
Port  Flags  State  Priority  Key  Number  State
-----
Gi0/1  SA    bndl  4096    0x3  0x1    0x3d
Gi0/2  SA    bndl  4096    0x3  0x2    0x3d
Gi0/3  SA    bndl  4096    0x3  0x3    0x3d
Partner information:
          LACP port
Port  Flags  Priority  Dev ID  Oper  Port  Port
          Key  Number  State
-----
Gi0/1  SA    61440  00d0.f800.0002  0x3  0x1  0x3d
Gi0/2  SA    61440  00d0.f800.0002  0x3  0x2  0x3d
Gi0/3  SA    61440  00d0.f800.0002  0x3  0x3  0x3d
    
```

Field	Description
Local information	Displays the local LACP information.
Port	Displays the system port ID.
Flags	Displays the port state flag: "S" indicates that the LACP is stable and in the state of periodically sending the LACPPDU; "A" indicates that the port is in the active mode.
State	Show the port aggregation information: "bndl" indicates that the port is aggregated; "Down" represents the disconnection port state; "susp" indicates that the port is not aggregated.
LACP Port Priority	Displays the LACP port priority.
Oper Key	Displays the port operation key.
Port Number	Displays the port number.
Port State	Displays the flag bit for the LACP port state.
Partner information	Partly Displays the LACP information of the peer port.
Dev ID	Partly Displays the system MAC information of the peer device.

Related Commands

Command	Description
port-group key mode	Enables the LACP on the port and specifies the aggregation group ID and operation mode.

Platform N/A

Description

3.19 show load-balance-profile

Use this command to display the enhanced profile.

show load-balance-profile [*profile-name*]

Parameter	Parameter	Description
Description	<i>profile-name</i>	Specifies the profile name.

Defaults -

Command Any mode.

Mode

Usage Guide All enhanced profiles are displayed if the profile name is not specified.

Configuration The following example displays the enhanced profile of LACP AP 3..

Examples

```
Ruijie(config)# show lacp summary 3
System Id:32768, 00d0.f8fb.0002
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs.
A - Device is in active mode.      P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper   Port   Port
Port   Flags   State  Priority   Key   Number  State
-----
Gi0/1   SA     bndl   4096      0x3   0x1     0x3d
Gi0/2   SA     bndl   4096      0x3   0x2     0x3d
Gi0/3   SA     bndl   4096      0x3   0x3     0x3d
Partner information:
          LACP port
Port   Flags   Priority  Dev ID   Oper   Port   Port
          Key   Number   State
-----
Gi0/1   SA     61440   00d0.f800.0002  0x3   0x1   0x3d
Gi0/2   SA     61440   00d0.f800.0002  0x3   0x2   0x3d
Gi0/3   SA     61440   00d0.f800.0002  0x3   0x3   0x3d
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description**3.20 trill field**

Use this command to configure the load balance mode of TRILL packets for a specified profile. Use the **no** form of this command to restore the default setting.

trill field [**vlan**] [**src-mac**] [**dst-mac**]

no mpls field

Parameter	Parameter	Description
Description	vlan	Load balance based on the VLAN ID of the TRILL packet.
	src-mac	Load balance based on the source MAC address of the TRILL packet.
	dst-mac	Load balance based on the destination MAC address of the TRILL packet.

Defaults The default load balance mode is **src-mac**, **dst-mac** and **vlan**.

Command Load balance template configuration mode

Mode

Usage Guide You need to configure the load balance profile first.

Configuration Examples The following example sets the load balance mode of TRILL packets for profile apl to **src-mac** and **src-port**.

```
Ruijie(config)# load-balance-profile apl
Ruijie(config-load-balance-profile)# trill field src-mac src-port
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4 VLAN Commands

4.1 add

Use this command to add one or a group Access interface into current VLAN. Use the **no** or **default** form of the command to remove the Access interface.

add interface { *interface-id* | **range** *interface-range* }

no add interface { *interface-id* | **range** *interface-range* }

default add interface { *interface-id* | **range** *interface-range* }

Parameter Description	Parameter	Description
	<i>interface-id</i>	Layer-2 Ethernet interface or layer-2 AP port.
	range <i>interface-range</i>	Range of the Layer-2 Ethernet interface or layer-2 AP port.

Defaults All layer-2 Ethernet interfaces are in the VLAN1.

Command mode VLAN configuration mode.

Usage Guide This command is only valid for the access port.

The configuration of this command is the same as specifying the VLAN to which interface belongs in the interface configuration mode (that is the **switchport access vlan** *vlan-id* command). For the two commands of adding the interface to the VLAN, the command configured later will overwrite the one configured before and take effect.

The configuration of adding the layer-2 AP into current VLAN through this command will only take effect for the layer-2 AP port, but not for the member port of the layer-2 AP port.

Configuration Examples The following example adds the interface GigabitEthernet 0/10 to VLAN20.

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
Ruijie# show interface GigabitEthernet 0/10 switchport
Interface  Switchport  Mode  Access  Native  Protected  VLAN lists
-----  -
GigabitEthernet 0/10  enabled  ACCESS  20    1    Disabled  ALL
```

The following example adds the interface range GigabitEthernet 0/1-10 to VLAN200.

```
Ruijie# configure terminal
SwitchA(config)#vlan 200
SwitchA(config-vlan)#add interface range GigabitEthernet 0/1-10
Ruijie# show vlan
```



```
SwitchA#show vlan
VLAN Name          Status          Ports
-----
1 VLAN0001         STATIC        Gi0/11,Gi0/12,Gi0/13,Gi0/14,Gi0/15,
Gi0/16,Gi0/17,Gi0/18,Gi0/19,Gi0/20,Gi0/21, Gi0/22, Gi0/23, Gi0/24
200 VLAN0200       STATIC        Gi0/1,Gi0/2,Gi0/3,Gi0/4,Gi0/5,
Gi0/6,Gi0/7,Gi0/8,Gi0/9,Gi0/10
```

The following example adds the AggregatePort10 to VLAN20.

```
Ruijie# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface aggregateport 10
Ruijie# show interface aggregateport 10 switchport
Interface Switchport Mode Access Native Protected VLAN lists
-----
AggregatePort 10 enabled ACCESS 20 1 Disabled ALL
```

Related Commands

Command	Description
show interface <i>interface-id</i> switchport	Displays the layer-2 interfaces.

Platform N/A

Description

4.2 name

Use this command to specify the name of a VLAN. Use the **no** or **default** form of this command to restore the default setting.

name *vlan-name*

no name

default name

Parameter Description

Parameter	Description
<i>vlan-name</i>	VLAN name

Defaults

The default name of a VLAN is the combination of "VLAN" and VLAN ID, for example, the default name of the VLAN 2 is "VLAN0002".

Command mode

VLAN configuration Mode.

Usage Guide

N/A

Configuration The following example sets the name of VLAN to 10.

Examples

```
Ruijie(config)# vlan 10
Ruijie(config-vlan)# name vlan10
```

Related Commands	Command	Description
		show vlan

Platform N/A

Description

4.3 show vlan

Use this command to display member ports of the VLAN.

show vlan [id *vlan-id*]

Parameter Description	Parameter	Description
		<i>vlan-id</i>

Defaults N/A

Command mode All modes

Usage Guide N/A

Configuration The following command displays the status of VLAN 1.

Examples

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                Status    Ports
-----
20 VLAN0020              STATIC   Gi0/1
```

Related Commands	Command	Description
	name	VLAN name.
	switchport access	Adds the interface to a VLAN.

Platform N/A

Description

4.4 switchport access

Use this command to configure an interface as a static access port and assign it to a VLAN. Use the **no** or **default** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

default switchport access vlan

Parameter Description	Parameter	Description
	<i>vlan-id</i>	The VLAN ID at which the port to be added.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command mode Interface configuration mode.

Usage Guide Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN. If the port is a trunk port, the operation does not take effect.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport access vlan 2
```

Related Commands	Command	Description
	switchport mode	Specifies the interface as Layer 2 mode (switch port mode).
	switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description N/A

4.5 switchport hybrid allowed

Use this command to add the port to the VLAN or remove the port from the VLAN, Use the **no** or **default** form of this command to restore the default setting.

switchport hybrid allowed vlan { { [**add** | **only**] **tagged** *vlist* | [**add**] **untagged** *vlist* } | **remove** *vlist* }

no switchport hybrid allowed vlan

default switchport hybrid allowed vlan

Parameter Description	Parameter	Description
	add	Adds the port to the VLAN.
	only	Adds the port to the VLAN and removes the port from the VLANs not on the VLAN list.
	tagged	Adds the port to the VLAN and the VLAN packets going out on the port are tagged with VLAN ID.
	untagged	Adds the port to the VLAN and the VLAN packets going out on the port are not tagged with VLAN ID.
	remove	Removes the port from the VLAN.
	<i>vlist</i>	Specifies the VLAN.

Defaults By default, the hybrid port is in all VLANs. All VLAN packets (except native VLAN packets) going out on the port are tagged with VLAN ID. Native VLAN packets are not tagged with VLAN ID.

Command mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example adds the hybrid port to VLAN 20 and VLAN 30 and the VLAN packets going out on the port are not tagged with VLAN ID.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged
20
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan add
untagged 30
```

The following example adds the hybrid port to VLAN 40 and VLAN 50 and the VLAN packets going out on the port are tagged with VLAN ID,

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged
40
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged
50
```

The following example removes the hybrid port from VLAN 20.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed
vlan remove 20
```

The following example adds the hybrid port to VLAN 20 and deletes all the other VLANs. The VLAN packets going out on the port are tagged with VLAN ID.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid allowed
vlan only tagged 20
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

4.6 switchport hybrid native

Use this command to configure the native VLAN for the hybrid port. Use the **no** or **default** form of this command to restore the default setting.

switchport hybrid native vlan *vlan-id*

no switchport hybrid native vlan

default switchport hybrid native vlan

Parameter Description

Parameter	Description
<i>vlan-id</i>	Configures the native VLAN for the hybrid port.

Defaults The default is VLAN 1.

Command mode Interface configuration mode

Usage Guide Native VLAN packets going out on the hybrid port are not tagged with VLAN ID. Packets not tagged with VLAN ID coming in on the hybrid port are taken as native VLAN packets.

Configuration Examples The following example configures VLAN 20 as the native VLAN for hybrid port GigabitEthernet 0/1.

```
Ruijie(config-if-GigabitEthernet 0/1)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)#switchport hybrid native
vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

4.7 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or a servicechain port. Use the **no** or **default** form of this command to restore the default setting.

switchport mode { **access** | **trunk** | **hybrid** | **uplink** | **servicechain** }

no switchport mode

default switchport mode

Parameter Description	Parameter	Description
	access	Configures the switch port as an access port.
	trunk	Configures the switch port as a trunk port.
	hybrid	Configures the switch port as a hybrid port.
	uplink	Configures the switch port as an uplink port.
	servicechain	Configures the switch port as a servicechain port.

Defaults By default, the switch port is an access port.

Command mode Interface configuration mode.

Usage Guide If a switch port is an access port, the port can be added only to one VLAN. You can run the **switchport access vlan** command to specify the VLAN to which the port belongs.

If a switch port is a trunk port, the port is added to all VLANs by default. You can also run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.

If a switch port is an uplink port, the port is added to all VLANs by default. Different from the trunk port, the uplink port sends packets with a tag carried, that is, the tag of packets from default VLANs will not be deleted. You can run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.

If a switch port is a hybrid port, the port is added to all VLANs by default. Different from a trunk port, a hybrid port can be added to a VLAN in tag or untag mode by running the **switchport hybrid allowed** command.

If a switch port is a servicechain port, the port does not need to learn MAC addresses and can forward packets from any VLAN. Note that before setting a switch port to a servicechain port, clear other configurations on the port and switches the port to an access port.

Configuration The following example configures port 1 as an access port.

Examples

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)#switchport mode access
```

The following example configures port 1 as a trunk port.

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

The following example configures port 1 as an uplink port.

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode uplink
```

The following example configures port 1 as a hybrid port.

```
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
```

The following example configures port 1 as a servicechain port.

```
Ruijie(config)#default int g 0/1
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode servicechain
```

Related Commands

Command	Description
switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform N/A
Description

4.8 switchport trunk allowed vlan

Use this command to add the trunk/uplink port to the VLAN or remove a trunk/uplink port from the VLAN. Use the **no** or **default** form of the command to restore the default setting.

switchport trunk allowed vlan { all | { add *vlan-list* | remove *vlan-list* | except *vlan-list* | only *vlan-list* } }

no switchport trunk allowed vlan

default switchport trunk allowed vlan

Parameter Description

Parameter	Description
all	Adds the trunk/uplink port to all VLANs.
add	Adds the trunk/uplink port to the VLAN.
remove	Removes the trunk/uplink port from the VLAN port.
except	Removes the trunk/uplink port from the VLAN and adds the port to all the other VLANs.
only	Adds the trunk/uplink port to the specified VLAN and removes the port from the VLANs not on the VLAN list.

<i>vlan-list</i>	Specifies the VLAN.
------------------	---------------------

Defaults The trunk/uplink port is in all VLANs by default.

Command mode Interface configuration mode.

Usage Guide A trunk/uplink port transmits all VLAN (1-4094) data by default. You can block some VLAN data by configuring this command. Use the **show interfaces** command to display configuration.

Configuration Examples The following example removes trunk port GigabitEthernet 0/10 from VLAN 2.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove
2
```

The following example removes trunk port GigabitEthernet 0/10 from VLAN 2.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except
10
```

The following example removes uplink port GigabitEthernet 0/10 from VLAN 10.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove
10
```

The following example adds uplink port GigabitEthernet 0/10 to all VLANs except VLAN10.

```
Ruijie(config)# interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed
vlan except 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.9 switchport trunk native vlan

Use this command to configure the native VLAN for the trunk/uplink port. Use the **no** or **default** form of this command to restore the default setting.

switchport trunk native vlan *vlan-id*
no switchport trunk native vlan
default switchport trunk native vlan

Parameter Description	Parameter	Description
	<i>vlan-id</i>	Native VLAN ID.

Defaults By default, the native VLAN for the trunk/uplink port is VLAN 1.

Command mode Interface configuration mode

Usage Guide After this function is enabled, packets not tagged with VLAN ID are taken as native VLAN packets. Tags are removed from native VLAN packets going out on the trunk port.

Configuration Examples The following example configures VLAN 10 as the native VLAN for trunk port GigabitEthernet 0/10.

```
Ruijie(config)#interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

The following example configures VLAN 10 as the native VLAN for unlinlink port GigabitEthernet 0/10.

```
Ruijie(config)#interface gigabitEthernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.10 vlan

Use this command to enter the VLAN configuration mode. Use the **no** or **default** form of this command to restore the default setting.

vlan { *vlan-id* | **range** *vlan-range* }
no vlan { *vlan-id* | **range** *vlan-range* }
default vlan { *vlan-id* | **range** *vlan-range* }

Parameter Description	Parameter	Description
	<i>vlan-id</i>	VLAN ID

	Default VLAN (VLAN 1) cannot be removed.
<i>vlan-range</i>	VLAN ID range.

Defaults The default is static VLAN.

Command mode Global configuration mode.

Usage Guide N/A

Configuration The following example creates VLAN 10.

Examples

```
Ruijie(config)# vlan 10
Ruijie(config-vlan)#
```

Related Commands	Command	Description
	show vlan	Displays member ports of the VLAN.

Platform Description N/A

5 MAC VLAN Commands

5.1 mac-vlan enable

Use this command to enable the MAC VLAN function on the port.

Use the **no** form or **default** form of this command to restore the default setting.

mac-vlan enable

no mac-vlan enable

default mac-vlan enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, MAC VLAN is disabled.

Command mode Interface configuration mode

Usage Guide The MAC VLAN entries configured globally will not take effect on the port unless the MAC VLAN function is enabled on this port.
The MAC VLAN function can be enabled on the hybrid port only.

Configuration The following example enables MAC VLAN.

Examples Ruijie(config-if-interface-id)# mac-vlan enable

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.2 mac-vlan mac-address

Use this command to configure the static MAC VLAN entries.

Use the **no** form or **default** form of this command to restore the default setting.

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri_val*]

no mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri_val*]

default mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri_val*]

Parameter Description	Parameter	Description
	<i>mac-address</i>	Specifies the MAC address.
	<i>mac-mask</i>	Specifies the MAC address mask, with the high bits being all 1 in binary. This field is full of F by default.
	<i>vlan-id</i>	Specifies the VLAN corresponding to the MAC address. The range is from 1 to 4,094.
	<i>pri_val</i>	Specifies the 802.1p priority of the VLAN corresponding to the MAC address. The range is from 0 to 7. The default value is 0.

Defaults No static MAC VLAN entry is configured by default.

Command mode Global configuration mode

Usage Guide Use this command to configure a static MAC VLAN entry including the MAC address, VLAN ID and VLAN priority. Use the **no** form of this command to remove the static MAC VLAN entry.

Configuration The following example configures a static MAC VLAN entry.

Examples

```
Ruijie(config)# mac-vlan mac-address 0001.0001.0001 vlan 100 priority 3
Ruijie(config)# mac-vlan mac-address 0002.0002.0000 mask ffff.ffff.0000 vlan 200 priority 5
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.3 show mac-vlan

Use this command to display the MAC VLAN entries.

```
show mac-vlan { all | dynamic | static | vlan vlan-id | mac-address mac-address [ mask mac-mask ] }
```

Parameter Description	Parameter	Description
	all	Displays all MAC VLAN entries.
	dynamic	Displays the dynamic MAC VLAN entries.
	static	Displays the static MAC VLAN entries.
	mac-address mac-address	Displays the MAC VLAN entry of the specified MAC address.
	mask mac-mask	Displays the MAC VLAN entry of the specified MAC address range.

vlan vlan-id	Displays the MAC VLAN entries of the specified VLAN.
---------------------	--

Defaults N/A

Command mode All configuration modes

Usage Guide If the **mac-address** parameter is specified without the **mask** parameter, the MAC-VLAN entry of the single MAC address is displayed.
If parameters both of **mac-address** and **mask** are specified, the MAC-VLAN entries in the specified MAC address range are displayed.

Configuration Examples The following example displays all MAC VLAN entries.

```
Ruijie# show mac-vlan all
The following MAC VLAN addresses exist:
S: Static   D: Dynamic
MAC ADDR          MASK                VLAN ID   PRIO   STATE
-----
0011.1100.0000    ffff.ff00.0000     100      1     S
0022.2222.0000    ffff.ffff.0000     200      2     S
0000.0000.0003    ffff.ffff.ffff     300      3     D
0000.0000.0004    ffff.ffff.ffff     400      4     D
0000.0000.0005    ffff.ffff.ffff     500      5     S&D
0000.0000.0006    ffff.ffff.ffff     600      6     S
0000.0000.0007    ffff.ffff.ffff     700      7     S&D
Total MAC VLAN address count: 7
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.4 show mac-vlan interface

Use this command to display the interfaces which are enabled with MAC VLAN.

show mac-vlan interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode All configuration modes

Usage Guide Use this command to verify whether the MAC VLAN function is enabled on the interface.

Configuration The following example displays the interfaces which are enabled with MAC VLAN.

Examples

```
Ruijie# show mac-vlan interface
MAC VLAN is enabled on following interface:
-----
fastethernet 0/3
fastethernet 0/10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6 Super-VLAN Commands

6.1 proxy-arp

Use this command to enable the proxy ARP function for a VLAN. Use the **no** form of this command to disable this function. Use the **default** form of this command to restore the default setting.

proxy-arp

no proxy-arp

default proxy-arp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command mode VLAN configuration Mode.

Usage Guide Super VLAN and sub VLAN must be both enabled with proxy ARP.

Configuration Examples The following example enables the proxy ARP function for VLAN 3.

```
Ruijie(config)# vlan 3
Ruijie(config-vlan)# proxy-arp
```

The following example disables the proxy ARP function for VLAN 3.

```
Ruijie(config)# vlan 3
Ruijie(config-vlan)# no proxy-arp
```

Related Commands	Command	Description
	show supervlan	Displays the super VLAN information.

Platform N/A

Description

6.2 show supervlan

Use this command to display the configuration of the super VLAN and its sub VLANs.

show supervlan

show supervlan id *vlan-id*

Parameter Description	Parameter	Description
		<i>vlan-id</i>

Defaults N/A

Command mode Any mode

Usage Guide N/A

Configuration The following example displays the configuration of super VLAN 2.

Examples

```
SwitchA(config-if-range)# show supervlan 2
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip
range
-----
          2          ON          10          ON          192.168.196.10 -
192.168.196.50
                                20          ON          192.168.196.60 -
192.168.196.100
                                30          ON          192.168.196.110 -
192.168.196.150
```

The following example displays the configuration of all super VLANs.

```
SwitchA(config-if-range)# show supervlan
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip
range
-----
          2          ON          10          ON          192.168.196.10 -
192.168.196.50
                                20          ON          192.168.196.60 -
192.168.196.100
                                30          ON          192.168.196.110 -
192.168.196.150
          6          ON          7          ON
                                8          ON
```

Related Commands	Command	Description
		N/A

Platform Description N/A

6.3 subvlan

Use this command to set the sub VLAN for the super VLAN. Use the **no** form of this command to disable this function. Use the **default** form of this command to restore the default setting.

subvlan *vlan-id-list*

no subvlan [*vlan-id-list*]

default subvlan [*vlan-id-list*]

Parameter Description	Parameter	Description
	<i>vlan-id-list</i>	Sub VLAN ID of the VLAN. Multiple VLANs are supported.

Defaults No super VLAN is set by default.

Command mode VLAN configuration Mode.

Usage Guide Use the **no subvlan** command to delete all sub VLANs of this super VLAN.

Configuration The following example sets the sub VLAN.

Examples

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#supervlan
SwitchA(config-vlan)#subvlan 10,20,30
```

Related Commands	Command	Description
	show supervlan	Displays the super VLAN information.

Platform N/A

Description

6.4 subvlan-address-range

Use this command to set the IP address range of the sub VLAN. Use the **no** form of this command to disable this function. Use the **default** form of this command to restore the default setting.

subvlan-address-range *start-ip end-ip*

no subvlan-address-range

default subvlan-address-range

Parameter Description	Parameter	Description
	<i>start-ip</i>	The start IP address of this sub VLAN
	<i>end-ip</i>	The end IP address of this sub VLAN

Defaults No IP address range is set by default.

Command mode VLAN configuration Mode.

Usage Guide N/A

Configuration The following example sets the IP address range for the sub VLAN.

Examples

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)#subvlan-address-range 192.168.23.1 192.168.23.5
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform N/A

Description

6.5 supervlan

Use this command to set the VLAN as a super VLAN. Use the **no** form of this command to disable this function. Use the **default** form of this command to restore the default setting.

supervlan

no supervlan

default supervlan

Parameter Description

Parameter	Description
N/A	N/A

Defaults No super VLAN is set by default.

Command mode VLAN configuration Mode.

Usage Guide By default, the super VLAN function is disabled.
No physical port can be added to a super VLAN.
Once a VLAN is not a super VLAN, all its sub VLANs become common static VLANs.

Configuration The following example configures a Sub VLAN.

Examples

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)#supervlan
```

Related Commands	Command	Description
	<code>show supervlan</code>	Displays the super VLAN information.

Platform N/A

Description

7 Protocol VLAN Commands

7.1 protocol-vlan ipv4 (in interface configuration mode)

Use this command to enable subnet VLAN. Use the **no** form of this command to restore the default setting.

protocol vlan ipv4

no protocol vlan ipv4

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Interface configuration mode.

Usage Guide An interface must work in Trunk/Hybrid mode.

Configuration The following example enables the subnet VLAN.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)# protocol-vlan ipv4
```

Related Commands	Command	Description
	no protocol-vlan ipv4	N/A

Platform N/A
Description

7.2 protocol-vlan ipv4 (in global configuration mode)

Use this command to configure VLAN for the specified subnet.

protocol-vlan ipv4 addr mask addr vlan id

Use this command to remove VLAN configuration for the specified subnet.

no protocol-vlan ipv4 addr mask addr

Use this command to remove VLAN configuration for all subnets.

no protocol-vlan ipv4

Parameter Description	Parameter	Description
	<i>addr</i>	IP address in the x.x.x.x format.
	<i>id</i>	VLAN ID, the maximal VLAN the product supports

Defaults It is disabled by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures VLAN 100 for the specified subnet.

```
Ruijie(config)# protocol-vlan ipv4 192.168.100.3 mask 255.255.255.0 vlan 100
```

Platform Description N/A

7.3 protocol-vlan profile (in global configuration mode)

Use this command to configure the profile for the VLAN.

protocol-vlan profile *num* **frame-type** *type* **ether-type** *type*

protocol-vlan profile *num* **frame-type** **LLC DSAP** *value* **SSAP** *value*

Use this command to delete the specified profile.

no protocol-vlan profile *num*

Use this command to delete all profiles.

no protocol-vlan profile

Parameter Description	Parameter	Description
	<i>num</i>	Profile indexes
	<i>type</i>	Type of message and Ethernet
	<i>value</i>	Service access point type.

Defaults It is disabled by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration The following example configures the profile for the VLAN.

Examples

```
Ruijie(config)# protocol-vlan profile 1 frame-type ETHERII ether-type aarp
Ruijie(config)# protocol-vlan profile 2 frame-type LLC DSAP 255 SSAP 255
```

Related Commands	Command	Description
	show protocol-vlan profile	N/A
	show protocol-vlan profile <i>num</i>	N/A
	no protocol-vlan profile	N/A
	no protocol-vlan profile <i>num</i>	N/A

Platform N/A

Description

7.4 protocol-vlan profile (in interface configuration mode)

Use this command to apply some profile to an interface.

protocol-vlan profile *num* vlan *id*

Use this command to clear the specified profile on the port.

no protocol-vlan profile *id*

Use this command to clear all profiles on the port.

no protocol-vlan profile

Parameter Description	Parameter	Description
	<i>num</i>	Profile indexes
	<i>id</i>	VLAN ID, the maximal VLAN the product supports.

Defaults This function is disabled by default.

Command mode Interface EXEC mode.

Usage Guide N/A

Configuration The following example applies profile 1 to VLAN 101.

Examples

```
Ruijie(config-if)# protocol-vlan profile 1 vlan 101
```

Related Commands	Command	Description
	show protocol-vlan profile	N/A
	show protocol-vlan profile <i>num</i>	N/A
	no protocol-vlan profile	N/A

no protocol-vlan profile <i>num</i>	N/A
--	-----

Platform N/A

Description

7.5 show protocol-vlan

Use this command to display a protocol VLAN.

show protocol-vlan [**profile** [*id*] | **ipv4**]

Parameter Description	Parameter	Description
	<i>id</i>	Profile index.

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the configuration of protocol VLAN.

```
Ruijie#show protocol-vlan

ip          mask          vlan
-----
1.2.1.0    255.255.255.0  5

interface   ipv4 status
-----
Gi0/1       enable

profile frame-type      ether-type/DSAP+SSAP  interface  vlan
-----
1          ETHERII             0x5fa      Gi0/1     12
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

8 Private VLAN Commands

8.1 debug bridge pvlan

Use this command to enable private VLAN debugging. Use the **no** or **default** form of this command to restore the default setting.

debug bridge pvlan



no debug bridge pvlan

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Debugging is disabled by default.

Command mode Privileged EXEC mode

Usage Guide Debugging information includes error and prompt messages appearing during private VLAN configuration.
This command can be used to troubleshoot VLAN and interface configuration failure.

-  With private VLAN debugging enabled, all super VLAN configuration and packet processing on SVI is displayed.
-  Debugging information helps troubleshooting and fault location.

Configuration The following example enables private VLAN debugging.

Examples Ruijie# debug bridge pvlan

The following example disables private VLAN debugging.

Ruijie# no debug bridge pvlan

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.2 private-vlan

Use this command to configure the private VLAN feature. Use the **no** or **default** form of this

command to restore the default setting.

private-vlan { community | isolated | primary }
no private-vlan { community | isolated | primary }
default private-vlan { community | isolated | primary }

Parameter Description	Parameter	Description
	community	Sets the community VLAN.
	isolated	Sets the isolated VLAN.
	primary	Sets the primary VLAN.

Defaults No private VLAN feature is configured by default.

Command mode VLAN configuration mode

Usage Guide N/A

Configuration Examples The following example configures the private VLAN feature.

```
Ruijie(config)#vlan 90
Ruijie(config-vlan)#private-vlan primary
Ruijie(config-vlan)#vlan 91
Ruijie(config-vlan)#private-vlan isolated
Ruijie(config-vlan)#vlan 92
Ruijie(config-vlan)#private-vlan community
```

The following example disables the private VLAN feature using the **no private-vlan** command.

```
Ruijie(config)#vlan 90
Ruijie(config-vlan)#no private-vlan primary
Ruijie(config-vlan)#vlan 91
Ruijie(config-vlan)#no private-vlan isolated
Ruijie(config-vlan)#vlan 92
Ruijie(config-vlan)#no private-vlan community
```

The following example disables the private VLAN feature using the **default private-vlan** command.

```
Ruijie(config)#vlan 90
Ruijie(config-vlan)#default private-vlan primary
Ruijie(config-vlan)#vlan 91
Ruijie(config-vlan)#default private-vlan isolated
Ruijie(config-vlan)#vlan 92
Ruijie(config-vlan)#default private-vlan community
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

8.3 private-vlan association

Use this command to associate the secondary VLAN with the primary VLAN on layer 2. Use the **no** or **default** form of this command to restore the default setting.

private-vlan association { *svlist* | **add** *svlist* | **remove** *svlist* }
no private-vlan association
default private-vlan association

Parameter Description	Parameter	Description
	<i>svlist</i>	The secondary VLAN list
	add <i>svlist</i>	Adds the associated secondary VLAN.
	remove <i>svlist</i>	Removes the associated secondary VLAN.

Defaults This function is disabled by default.

Command mode VLAN configuration Mode.

Usage Guide N/A

Configuration Examples The following example associates the secondary VLAN with the primary VLAN on layer 2.

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan association add 24-26
```

The following example removes the association between the secondary VLAN with the primary VLAN.

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan association remove 24
```

Related Commands	Command	Description
	show vlan private-vlan	N/A

Platform N/A
Description

8.4 private-vlan mapping

Use this command to associate the secondary VLAN with the primary VLAN on layer 3. Use the **no** or

default form of this command to restore the default setting.
private-vlan mapping { *svlist* | **add** *svlist* | **remove** *svlist* }
no private-vlan mapping
default private-vlan mapping

Parameter Description	Parameter	Description
	<i>svlist</i>	Secondary VLAN list.
	add <i>svlist</i>	Adds the associated secondary VLAN.
	remove <i>svlist</i>	Removes the associated secondary VLAN.

Defaults This function is disabled by default.

Command mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example associates the secondary VLAN with the primary VLAN on layer 3.

```
Ruijie(config)# interface vlan 22
Ruijie(config-if)# private-vlan mapping add 24-26
```

Related Commands	Command	Description
	show vlan private-vlan	N/A

Platform Description N/A

8.5 show vlan private-vlan

Use this command to display the private VLAN configuration.

show vlan private-vlan [**community** | **primary** | **isolated**]

Use this command to display all the private VLANs configuration.

show vlan private-vlan

Parameter Description	Parameter	Description
	primary	Displays the primary VLAN information.
	community	Displays the community VLAN information.
	isolated	Displays the isolated VLAN information.

Defaults N/A

Command mode All modes

Usage Guide N/A

Configuration The following example displays the private VLAN configuration.

Examples

```
Ruijie# show vlan private-vlan
```

VLAN	Type	Status	Routed	Ports	Associated VLANs
30	primary	inactive	Enabled		
31	isolated	inactive	Disabled		No Association
90	primary	active	Disabled		91-92
91	isolated	active	Disabled		90
92	community	active	Disabled	Gi0/1	90

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

8.6 switchport mode private-vlan

Use this command to declare the private VLAN mode of the interface. Use the **no** or **default** form of this command to restore the default setting.

switchport mode private-vlan { host | promiscuous }

no switchport mode

default switchport mode

Parameter Description

Parameter	Description
host	Host mode of the private VLAN
promiscuous	Promiscuous mode of the private VLAN

Defaults The port is an access port by default.

Command mode Interface configuration mode.

Usage Guide Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode.

The port mode must be configured as the promiscuous mode.

Configuration The following example applies the private host mode to the interface.

Examples

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode private-vlan host
```

The following example applies the promiscuous mode to the interface.

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#sw mode private-vlan promiscuous
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform N/A

Description

8.7 switchport private-vlan host-association

Use this command to associate the primary VLAN, which is associated with the private VLAN mode of the interface, with the secondary VLAN. Use the **no** or **default** form of this command to restore the default setting.

switchport private-vlan host-association *p_vid s_vid*

no switchport private-vlan host-association

default switchport private-vlan host-association

Parameter Description

Parameter	Description
<i>p_vid</i>	Primary VID.
<i>s_vid</i>	Secondary VID

Defaults This function is disabled by default.

Command mode Interface configuration mode.

Usage Guide Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode.

Whether a port is configured as an isolated port or community port depends on the *s_vid* parameter. *p_vid* and *s_vid* must be respectively the IDs of the primary VLAN and secondary VLAN in a PVLAN

pair, on which Layer-2 association is performed.

One host port can be associated with only one PVLAN pair.

Configuration The following example associates the secondary VLAN with the primary VLAN on the host port.

Examples

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode private-vlan host
Ruijie(config-if)# switchport private-vlan host-association 22 23
Ruijie(config-if)# default switchport private-vlan host-association
Ruijie(config-if)# switchport private-vlan host-association 22 25
```

**Related
Commands**

Command	Description
show vlan private-vlan	N/A

Platform N/A

Description

8.8 switchport private-vlan mapping

Use this command to configure the secondary VLAN for the promiscuous port. Use the **no** or **default** form of this command to restore the default setting.

switchport private-vlan mapping *p_vid* { *svlist* | **add** *svist* | **remove** *svlist* }

no switchport private-vlan mapping

default switchport private-vlan mapping

Parameter	Parameter	Description
Description	<i>p_vid</i>	Indicates the primary VLAN ID in a PVLAN pair.
	<i>svlist</i>	Indicates the secondary VLAN associated with a promiscuous port. Layer-2 association must be performed between it and <i>p_vid</i> .
	add	Adds a secondary VLAN to be associated with a port.
	remove	Cancels the secondary VLAN associated with a port.

Defaults This function is disabled by default.

Command mode Interface configuration mode

Usage Guide The port mode must be configured as the promiscuous mode.

Layer-2 association must be performed between the primary and secondary VLAN.

Configuration The following example configures the secondary VLAN for the promiscuous port.

Examples

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if)# switchport mode private-vlan
promiscuous
Ruijie(config-if)# switchport private-vlan mapping 22 add 23-25
```

**Related
Commands**

Command	Description
show vlan private-vlan	N/A

Platform

N/A

Description

9 Voice VLAN Commands

9.1 show voice vlan

Use this command to display the Voice VLAN configurations and the current state, including the working mode of the port with Voice VLAN enabled.

show voice vlan

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the Voice VLAN configurations and the current state.

Examples

```
Ruijie(config)# show voice vlan
Voice VLAN status: ENABLE           //Voice VLAN is enabled
Voice VLAN ID: 2                    //Voice VLAN ID
Voice VLAN security mode: Security  //Security Mode
Voice VLAN aging time: 5 minutes    //Aging Time
Voice VLAN cos: 6                   //Voice VLAN CoS
Voice VLAN dscp: 46                 //Voice VLAN DSCP
Current voice vlan enabled port mode: // Voice VLAN Enabled Port & Mode
PORT                                MODE
-----
Fa0/1                                Auto
```

Related Commands	Command	Description
	voice vlan <i>vlan-id</i>	Set a voice vlan.
	voice vlan aging <i>minutes</i>	Set the Voice VLAN aging time.
	voice vlan cos <i>cos-value</i>	Set the CoS value for the Voice VLAN.
	voice vlan dscp <i>dscp-value</i>	Set the DSCP value for the Voice VLAN.
	voice vlan enable	Enable the Voice VLAN.
	voice vlan mode auto	Set the Voice VLAN working mode.
	voice vlan security enable	Enable the Voice VLAN security mode.

Platform N/A

Description

9.2 show voice vlan oui

Use this command to display the OUI address, OUI mask and the description information.

show voice vlan oui

Parameter	Parameter	Description
Description	N/A	N/A

Defaults All modes.

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the OUI address.

Examples

```
Ruijie(config)# show voice vlan oui
OUI           Mask           Description
-----
0001.e300.0000 ffff.ff00.0000 Siemens phone
0003.6b00.0000 ffff.ff00.0000 Cisco phone
0004.0d00.0000 ffff.ff00.0000 Avaya phone
0060.b900.0000 ffff.ff00.0000 Philips/NEC phone
00d0.1e00.0000 ffff.ff00.0000 Pingtel phone
00e0.7500.0000 ffff.ff00.0000 Polycom phone
00e0.bb00.0000 ffff.ff00.0000 3com phone
```

The following lists the field description .

Field	Description
OUI	The OUI address, the source MAC address for the voice packet.
Mask	The OUI mask. The valid length for the OUI address.
Description	The description information for the OUI address.

Related Commands

Command	Description
voice vlan mac-address <i>mac-addr</i> mask <i>oui-mask</i> [description <i>text</i>]	Set the OUI address for the voice packet recognized by the Voice VLAN.

Platform N/A

Description

9.3 voice vlan

Use this command to enable Voice VLAN in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan *vlan-id*

no voice vlan

Parameter Description	Parameter	Description
	<i>vlan-id</i>	The Voice VLAN ID.

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide Use this command to enable the Voice VLAN and specify the Voice VLAN ID.

- i** 1. The corresponding VLAN shall be created before configuring the Voice VLAN; 2. The default VLAN is VLAN1 and cannot be set as the Voice VLAN; 3. A VLAN is not allowed to be set as the Voice VLAN and the Super VLAN at the same time; 4. With 802.1x VLAN auto-switching function enabled, the assigned VID shall not be set as the Voice VLAN ID; 5. RSPAN Remote VLAN and Voice VLAN cannot be the same VLAN, or it influences the remote port mirror and the Voice VLAN function.

Configuration The following example sets the VLAN2 as the Voice VLAN.

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

Related Commands	Command	Description
	show voice vlan	Display Voice VLAN configurations and the current state.

Platform N/A

Description

9.4 voice vlan aging

Use this command to set the Voice VLAN aging time in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan aging *minutes*

no voice vlan aging

Parameter Description	Parameter	Description
	<i>minutes</i>	The Voice VLAN aging time. Range: 5 to 10,000. Unit: minute.

Defaults The default is 1440 minutes.

Command mode Global configuration mode

Usage Guide If the device has not received any voice packets from the port within the aging time, this Voice VLAN will be removed from this port.

 The aging time is valid for the auto-mode only.

Configuration Examples The following example sets the Voice VLAN aging time to 10 minutes.

```
Ruijie(config)# voice vlan aging 10
```

Related Commands	Command	Description
	show voice vlan	Display Voice VLAN configurations and the current state.

Platform N/A

Description

9.5 voice vlan cos

Use this command to set the Voice VLAN CoS value in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan cos *cos-value*

no voice vlan cos

Parameter Description	Parameter	Description
	<i>cos-value</i>	The Voice VLAN CoS value. Range: 0 to 7.

- Defaults** The default is 6.
- Command mode** Global configuration mode
- Usage Guide** You can improve the Voice VLAN priority level and the session quality, by modifying the Voice VLAN CoS and DSCP value.

Configuration The following example sets the Voice VLAN CoS value to 5.

Examples

```
Ruijie(config)# voice vlan cos 5
```

Related Commands	Command	Description
		show voice vlan

Platform N/A

Description

9.6 voice vlan dscp

Use this command to set the Voice VLAN DSCP value in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan dscp *dscp-value*

no voice vlan dscp

Parameter Description	Parameter	Description
		<i>dscp-value</i>

Defaults The default is 46.

Command mode Global configuration mode

Usage Guide You can improve the Voice VLAN priority level and the session quality, by modifying the Voice VLAN CoS and DHCP value.

Configuration The following example sets the Voice VLAN DSCP value to 40.

Examples

```
Ruijie(config)# voice vlan dscp 40
```

Related Commands	Command	Description
		show voice vlan

	current state.
--	----------------

Platform N/A

Description

9.7 voice vlan enable

Use this command to enable the Voice VLAN DSCP value in the interface configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan enable


no voice vlan enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Interface configuration mode

Usage Guide Use this command to enable the Voice VLAN on the physical port only. The Voice VLAN can be enabled on the Access Port, Trunk Port, Hybrid Port, Private VLAN host port, Private VLAN promiscuous port and Uplink port on the Ruijie products.

 With the global Voice VLAN disabled, although the Voice VLAN can be enabled on the port, it is invalid.

Configuration Examples The following example enables the Voice VLAN function on the interface FastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

Related Commands	Command	Description
	show voice vlan	Display Voice VLAN configurations and the current state.

Platform N/A

Description

9.8 voice vlan mac-address

Use this command to set the recognizable Voice VLAN OUI address. Use the **no** form of this

command to restore the default setting.

voice vlan mac-address *mac-addr* **mask** *oui-mask* [**description** *text*]

no voice vlan mac-address *mac-addr*

**Parameter
Description**

Parameter	Description
<i>mac-addr</i>	In the format of <i>H.H.H</i> . The source MAC address for the voice packets.
<i>oui-mask</i>	In the format of <i>H.H.H</i> . The valid length for the OUI address.
<i>text</i>	The description for the OUI address.

Defaults


By default, no OUI has been configured.

**Command
mode**

Global configuration mode

Usage Guide

Use this command to identify the voice packets from different manufacturers. The first three bytes of the MAC address for the voice device are used to identify the manufacture. Voice VLAN determines whether the packets are voice packets or not through the OUI address obtained from the source MAC address and the OUI mask for the received packets.

 The Voice VLAN OUI address cannot be the multicast address and the configured mask shall be continuous.

**Configuration
Examples**

The following example sets the OUI address 0012.3400.0000 as the valid address for the Voice VLAN.

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description Company A
```

**Related
Commands**

Command	Description
show voice vlan oui	Display the OUI address, OUI address mask and the descriptions.

**Platform
Description**

N/A

9.9 voice vlan mode auto

Use this command to set the Voice VLAN auto mode. Use the **no** form of this command to disable this function.

voice vlan mode auto


no voice vlan mode auto


Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is in auto mode by default.

Command mode Interface configuration mode

Usage Guide The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.

-  1. With the Voice VLAN enabled on the port and in the manual mode, this port must be added to the Voice VLAN manually to ensure the function validity. 2. When the port works in the auto-mode, note that the native VLAN of the port cannot be set as the Voice VLAN for the normal function performance. 3. The Trunk Port/Hybrid Port on the Ruijie product can transmit the packets in all VLANs by default. First remove the Voice VLAN from the allowed VLAN list for the port, then enable the Voice VLAN to ensure that the port disconnecting with the voice device cannot be added to the Voice VLAN, or the port not used for a long time can be still in the Voice VLAN.

-  1. With the Voice VLAN enabled on the port, the auto and manual modes switchover is disallowed. Disable the Voice VLAN first if it is necessary to switch the modes. 2. In the auto mode, it fails to add/remove the port to/from the Voice Vlan by using the command.

Configuration Examples The following example sets the Voice VLAN on the interface FastEthernet 0/1 to work in the auto mode.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-vlan)# voice vlan mode auto
```

Related Commands	Command	Description
	show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

9.10 voice vlan security enable

Use this command to enable the Voice VLAN security mode in the global configuration mode. Use the **no** form of this command to disable this function.

voice vlan security enable


no voice vlan security enable


Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command mode Global configuration mode

Usage Guide The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.

 You are not recommended to transmit the voice and service data in the Voice VLAN at the same time. But if it is necessary for you, you shall ensure that the Voice VLAN security mode has been disabled.

 In the security mode, only the source MAC addresses for the untagged packets and the packets carried with Voice VLAN tag are checked. For other packets carried with non-voice vlan tag that free from the Voice VLAN security/normal mode, the devices forward or discard those packets according to the VLAN rule.

Configuration The following example enables the Voice VLAN security mode.

Examples

```
Ruijie(config)# voice vlan security enable
```

Related Commands	Command	Description
	show voice vlan	Display Voice VLAN configurations and the current state.

Platform Description N/A

10 MSTP Commands

10.1 bpdu src-mac-check

Use this command to enable the BPDU source MAC address check function on the interface. Use the **no** form of this command to restore the default setting.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

Parameter Description	Parameter	Description
	<i>H.H.H</i>	Indicates that only the BPDU messages from this MAC address are received.
	no	Indicate that the BPDU messages from any MAC address are received.

Defaults This function is disabled by default.

Command Interface configuration mode.

Mode

Usage Guide BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.

Configuration Examples The following example indicates only the BPDU with 00d0.f800.1e2f as the source MAC address will be received by interface Gi 1/1 .

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id-interface-id)# bpdu src-mac-check
00d0.f800.1e2f
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.2 bridge-frame forwarding protocol bpdu

Use this command to enable BPDU transparent transmission. Use the **no** form of this command to restore the default setting.

bridge-frame forwarding protocol bpdu
no bridge-frame forwarding protocol bpdu

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide In the IEEE 802.1Q standard, 01-80-C2-00-00-00, the destination MAC address of BPDU frames, is reserved. Devices following the IEEE 802.1Q standard don't forward BPDU frames. In real network deployment, devices may be required to support BPDU transparent transmission. For example, when a device is not enabled with STP, BPDU transparent transmission can help implement STP calculation.
 BPDU transparent transmission works only when STP is disabled.

Configuration The following example enables BPDU transparent transmission.

Examples Ruijie(config)# bridge-frame forwarding protocol bpdu

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.3 clear spanning-tree counters

Use this command to clear the statistics of the sent and received STP packets.

clear spanning-tree detected-protocols [interface *interface-id*]

Parameter Description	Parameter	Description
	<i>interface-id</i>	ID of the interface

Defaults N/A**Command Mode** Privileged EXEC mode**Usage Guide** It is used to clear the statistics of the sent and received STP packets.**Configuration** The following example clears the statistics of the sent and received STP packets.**Examples**

```
Ruijie# clear spanning-tree counters
```

The following example clears the statistics of the sent and received packets on interface Gi 0/1.

```
Ruijie# clear spanning-tree counters interface gigabitethernet 0/1
```

Related Commands

Command	Description
show spanning-tree counters	Displays the statistics of STP transceived packets.

Platform Description N/A

10.4 clear spanning-tree detected-protocols

Use this command to force the interface to send the RSTP BPDU message and check the BPDU messages.

clear spanning-tree detected-protocols [interface *interface-id*]

Parameter Description

Parameter	Description
<i>interface-id</i>	ID of the interface

Defaults N/A**Command Mode** Privileged EXEC mode**Usage Guide** Use this command to force the interface to send the RSTP BPDU message.**Configuration** Forces to check the version of all interfaces.**Examples**

```
Ruijie# clear spanning-tree detected-protocols
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the

	interface.
--	-------------------

Platform N/A

Description

10.5 clear spanning-tree mst topochange record

Use this command to clear STP topology change record.

clear spanning-tree mst *instance-id* topochange record

Parameter Description	Parameter	Description
		<i>instance-id</i>

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example clears STP topology change record.

Examples

```
Ruijie# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
Time                Interface          Old status   New status   Type
-----
2013.5.1 4:18:46   GI0/6         Learning    Forwarding   Normal
Ruijie# clear spanning-tree mst 0 topochange record
Ruijie# show spanning-tree mst 0 topochange record
%There's no topology change information has been record on mst 0.
```

Related Commands	Command	Description
		N/A

Platform N/A

Description

10.6 instance instance-id vlan vlan-range

Use this command to set instance and VLAN mapping relations. Use the **no** form of the command to restore the default setting.

instance *instance-id* **vlan** *vlan-range*
no instance *instance-id* { **vlan** *vlan-range* }

Parameter Description

Parameter	Description
<i>instance-id</i>	Instance ID, in the range from 0 to 64
<i>vlan-range</i>	VLAN range, in the range from 1 to 4094.

Defaults

The default is instance 0.

Command Mode

MST configuration mode

Usage Guide

instance *instance-id* **vlan** *vlan-range* : Add VLAN to MST instance. Instance-ID is in the range from 0 to 64 and VLAN is in the range from 1 to 4094. Use commas to separate VLAN IDs and use hyphen to indicate VLAN range, e.g., instance 10 vlan 2,3,6-9, which adds VLAN 2, 3, 4, 5, 6, 7, 8, 9 to instance 10. By default, all VLANs are in instance 0. Use the **no** form of this command to remove VLAN from instance 1-64.

If you create 64 instances by stacking on a Ruijie device with a small memory (e.g., 64M), the memory may be undersized. It is recommended to limit stacking instance number.

Configuration Examples

This example enters MST mode and maps VLAN 3 and 5-10 to MST instance1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 3, 5-10
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      :
Revision : 0
Instance  Vlans Mapped
-----  -
0         1-2,4,11-4094
1         3,5-10
-----  -
Ruijie(config-mst)# exit
Ruijie(config)#
```

The following example removes VLAN3 from instance 1.

```
Ruijie(config-mst)# no instance 1 vlan 3
```

The following example removes instance 1.

```
Ruijie(config-mst)# no instance 1
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

10.7 l2protocol-tunnel stp

Use this command to enable BPDU TUNNEL globally. Use the **no** form of this command to disable this function.

l2protocol-tunnel stp

no l2protocol-tunnel stp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Global configuration mode

Mode

Usage Guide If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.

Configuration The following example enables BPDU TUNNEL globally.

Examples

```
Ruijie(config)# l2protocol-tunnel stp
Ruijie(config)# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

10.8 l2protocol-tunnel stp enable

Use this command to enable BPDU TUNNEL on the interface. Use the **no** form of this command to disable this function.

l2protocol-tunnel stp enable

no l2protocol-tunnel stp enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.

Configuration The following example enables BPDU TUNNEL on the interface.

Examples

```
Ruijie(config-if-interface-id)# l2protocol-tunnel stp enable
Ruijie(config-if-interface-id)# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address: 01d0.f800.0005
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.9 l2protocol-tunnel stp tunnel-dmac

Use this command to configure the STP address for transparent transmission through BPDU TUNNEL. Use the **no** form of this command to restore the default setting.

l2protocol-tunnel stp tunnel-dmac *mac-address*

no l2protocol-tunnel stp tunnel-dmac

Parameter Description	Parameter	Description
	<i>mac-address</i>	The STP address for transparent transmission.

Defaults The default is 01d0.f800.0005.

Command Mode Global configuration mode

Usage Guide The available STP address includes 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.

Configuration The following example configures the STP address for transparent transmission through BPDU

Examples TUNNEL.

```
Ruijie(config)# l2protocol-tunnel stp tunnel-dmac 011a.a900.0005
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

10.10 name

Use this command to set MST name. Use the **no** form of the command to restore the default setting.

name *name*

no name

Parameter Description

Parameter	Description
<i>name</i>	MST name, up to 32 characters.

Defaults The default is NULL.

Command MST configuration mode

Mode

Usage Guide **name** *name*: Sets the MST name, up to 32 characters.

show spanning-tree mst configuration: Displays MST region information.

Configuration This example sets MST name to region1.

Examples

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# name region1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      : region1
Revision  : 0
Instance  Vlans Mapped
-----
0         : ALL
Ruijie(config-mst)# exit
Ruijie(config)#
```


Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

10.11 revision

Use this command to set revision number of MSTP region. Use the **no** form of the command to restore the default setting.

revision *version*

no revision

Parameter Description	Parameter	Description
	<i>version</i>	

Defaults

The default is 0.

Command Mode MST configuration mode

Usage Guide **revision** *version*: Sets the MST version, in the range from 0 to 65535.
show spanning-tree mst configuration: Displays MST region information.

Configuration This example sets revision number to 1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      :
Revision : 1
Instance  Vlans Mapped
-----
0          : ALL
Ruijie(config-mst)# exit
Ruijie(config)#
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

10.12 show l2protocol-tunnel stp

Use this command to display BPDU TUNNEL configuration.

show l2protocol-tunnel stp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode / Global configuration mode / Interface configuration mode

Usage Guide N/A

Configuration The following example displays BPDU TUNNEL configuration.

Examples

```
Ruijie# show l2protocol-tunnel stp

L2protocol-tunnel: stp Enable
L2protocol-tunnel destination mac address:011a.a900.0005
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

10.13 show spanning-tree

Use this command to display the global spanning-tree configuration.

show spanning-tree [summary | forward-time | hello-time | max-age | inconsistentports] tx-hold-count | pathcost method | max_hops | counters]

Parameter Description	Parameter	Description
	summary	Displays the information of MSTP instances and forwarding status of the interfaces.

inconsistentports	Displays the block port due to root guard or loop guard.
forward-time	Displays BridgeForwardDelay.
hello-time	Displays BridgeHelloTime.
max-age	Displays BridgeMaxAge.
max-hops	Displays the maximum hops of an instance.
tx-hold-count	Displays TxHoldCount.
pathcost method	Displays the method used for calculating path cost.
counters	Displays the statistics of STP transceived packets.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Mode

Usage Guide N/A

Configuration The following example displays the global spanning-tree configuration.

Examples Ruijie# show spanning-tree hello-time

The following example displays the sent and received STP packets.

```
Ruijie# show spanning-tree counters
----- STP BPDU count -----
Port                Receive      Send
GigabitEthernet 0/3      0           122594

----- STP TC or TCN count -----
MSTID   Port                Receive      Send
0       GigabitEthernet 0/3      0           0
```

Related Commands

Command	Description
spanning-tree pathcost method	Sets the pathcost method.
spanning-tree forward-time	Sets BridgeForwardDelay.
spanning-tree hello-time	Sets BridgeHelloTime.
spanning-tree max-age	Sets BridgeMaxAge.
spanning-tree max-hops	Sets the maximum hops of an instance.
spanning-tree tx-hold-count	Displays TxHoldCount.

Platform N/A

Description

10.14 show spanning-tree interface

Use this command to display the STP configuration of the interface, including the optional spanning tree.

show spanning-tree interface *interface-id* [{ **bpdufilter** | **portfast** | **bpduguard** | **link-type** }]

Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface ID
	bpdufilter	Displays the status of BPDU filter.
	portfast	Displays the status of portfast.
	bpduguard	Displays the status of BPDU guard.
	link-type	Displays the link type of an interface.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the STP configuration on interface Gi 0/1.

```
Ruijie# show spanning-tree int gi 0/1

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : None

##### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 32768.001a.a979.00ea
PortDesignatedCost : 0
PortDesignatedBridge :32768.001a.a979.00ea
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 200000
```

```
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
```

**Related
Commands**

Command	Description
spanning-tree bpdudfilter	Enables the BPDU filter feature someone the interface.
spanning-tree portfast	Enables the portfast on the interface.
spanning-tree bpduguard	Enables the BPDU guard on the interface.
spanning-tree link-type	Sets the link type of the interface to point-to-point.

Platform N/A**Description**

10.15 show spanning-tree mst

Use this command to display the information of MST and instances.

```
show spanning-tree mst { configuration | instance-id [ interface interface-id ] }
```

**Parameter
Description**

Parameter	Description
configuration	The MST configuration of the equipment.
<i>instance-id</i>	Instance number
<i>interface-id</i>	Interface number

Defaults All the instances are displayed by default.**Command
Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode**Usage Guide** N/A**Configuration** The following example displays the information of MST and instances.**Examples**

```
Ruijie# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      : test
Revision  : 0
Instance  Vlans Mapped
-----
0         : 2-4094
1         : 1
```

Field Description

Field	Description
Multi spanning tree protocol	Enables MSTP protocol.
Name	Name of the MST region
Revision	Revision of the MST region
Instance Vlans Mapped	Mapping relation between the instance and VLAN

Related Commands

Command	Description
spanning-tree mst configuration	Configures the MST region.
spanning-tree mst cost	Displays the path cost of the instance.
spanning-tree mst max-hops	Displays the maximum hops of the instance.
spanning-tree mst priority	Displays the equipment priority of the instance.
spanning-tree mst port-priority	Displays the port priority of the instance.

Platform N/A

Description

10.16 show spanning-tree mst topochange record

Use this command to display the STP topology change record.

show spanning-tree mst *instance-id* topochange record

Parameter Description

Parameter	Description
<i>instance-id</i>	Instance ID.

Defaults N/A

Command Mode Privileged EXEC mode / Global configuration mode / Interface configuration mode

Usage Guide N/A

Configuration The following example displays the STP topology change record of instance 0.

Examples

```
Ruijie# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
Time                Interface          Old status  New status  Type
-----
2013.5.1 4:18:46   GI0/6       Learning   Forwarding  Normal
```

Field	Description
-------	-------------

Time	The time when the topology changes.
Interface	The interface whose topology changes.
Old status	Old STP status on the interface.
New status	New STP status on the interface.
Type	Topology change may be caused by the following causes: Normal: UP/DOWN state change on the interface, LoopGuard Block: Loop-inconsistence causes the interface to be blocked. RootGuard Block: Root-inconsistence causes the interface to be blocked. Inferior Block: Receiving inferior BPDU frames causes the interface to be blocked. LoopGuard Unblock: The interface returns to Forward status from loop-inconsistence. RootGuard Unblock: The interface returns to Forward status from root-inconsistence. Inferior Unblock-The interface returns to Forward status after not receiving inferior BPDU frames.

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

10.17 spanning-tree

Use this command to enable MSTP and configure its basic settings globally. The **no** form of the command disables the spanning-tree function. The **no** form of the command with parameters only restores the corresponding parameters to the default values, but does not disable the spanning-tree function.

spanning-tree [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*]

no spanning-tree [**forward-time** | **hello-time** | **max-age**]

**Parameter
Description**

Parameter	Description
forward-time <i>seconds</i>	Interval at which the port status changes, in the range from 4 to 30 in the unit of seconds. The default is 15.
hello-time <i>seconds</i>	Interval at which the switch sends the BPDU message, in the range

	from 1 to 10 in the unit of seconds. The default is 2.
max-age <i>seconds</i>	Maximum aging time of the BPDU message, in the range from 6 to 40 in the unit of seconds. The default is 20.

Defaults This function is disabled by default.

Command Global configuration mode.

Mode

Usage Guide The values of **forward-time**, **hello time** and **max-age** are interrelated. Modifying one of these three parameters will affect the others. There is a restricted relationship among the above three values.
 $2 * (\text{Hello Time} + 1.0\text{snd}) \leq \text{Max-Age Time} \leq 2 * (\text{Forward-Delay} - 1.0\text{snd})$
 If the values do not according with the condition, the settings do not work.

Configuration The following example enables the spanning-tree function.

Examples

```
Ruijie(config)# spanning-tree
```


 The following example configures the BridgeForwardDelay.

```
Ruijie(config)# spanning-tree forward-time 10
```

Related Commands	Command	Description
	show spanning-tree	Displays the global STP configuration.
	spanning-tree mst cost	Sets the PathCost of an STP interface.
	spanning-tree tx-hold-count	Sets the global TxHoldCount of STP.

Platform N/A

Description

10.18 spanning-tree autoedge

Use this command to enable Autoedge on the interface. Use the **disabled** form of this command to disable this function.

spanning-tree autoedge [disabled]

Parameter Description	Parameter	Description
	disabled	Disabled Autoedge on the interface.

Defaults This function is enabled by default.

Command Interface configuration mode.

Mode

Usage Guide If the designated port of a device does not receive a BPDU from the downlink port within a specific

period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.

You can run the spanning-tree autoedge disabled command to disable Auto Edge.

Configuration The following example disables Autoedge on the interface.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id-interface-id)# spanning-tree autoedge disabled
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration information of the interface.

Platform N/A

Description

10.19 spanning-tree bpdudfilter

Use this command to enable BPDU filter on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU filter function on the interface.

spanning-tree bpdudfilter [enabled | disabled]

Parameter Description

Parameter	Description
enabled	Enables BPDU filter on the interface.
disabled	Disables BPDU filter on the interface.

Defaults This function is disabled by default,

Command Interface configuration mode.

Mode

Usage Guide If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Configuration The following example enables BPDU filter on interface Gi 1/1.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id-interface-id)# spanning-tree bpdudfilter enable
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform N/A

Description

10.20 spanning-tree bpduguard

Use this command to enable the BPDU guard function on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU guard function on the interface.

spanning-tree bpduguard [enabled | disabled]

Parameter Description

Parameter	Description
enabled	Enables BPDU guard on the interface.
disabled	Disables BPDU guard on the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide

1. If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
2. Run command **errdisable recovery [interval seconds]** to recover the interface in Error-disabled state.

Configuration Examples The following example enables the BPDU guard function on the interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id-interface-id)# spanning-tree bpduguard enable
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform N/A

Description

10.21 spanning-tree compatible enable

Use this command to send the message selectively carried with MSTI according to the interface attribute of current port to realize interconnection with other vendors. Use the **no** form of this command to restore the default setting.

spanning-tree compatible enable

no spanning-tree compatible enable

Parameter

Parameter	Description
-----------	-------------

Description		
	N/A	N/A

Defaults This function is disabled by default. .

Command Interface configuration mode.

Mode

Usage Guide If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between Ruijie devices and other SPs' devices.

Configuration The following example enables the compatibility mode on interface Gi 0/1.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id-interface-id)#spanning-tree compatible enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

10.22 spanning-tree guard loop

Use this command to enable **loop guard** on the interface to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the **no** form of this command to disable **loop guard**.

spanning-tree guard loop

no spanning-tree guard loop

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Interface configuration mode.

Mode

Usage Guide

1. Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.
2. The loop guard function and root guard function cannot be enabled at the same time.

Configuration The following example enables **loop guard** on interface Gi 0/1.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree guard loop
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

10.23 spanning-tree guard none

Use this command to disable **guard** on the interface. Use the **no** form of this command to enable this function

spanning-tree guard none

no spanning-tree guard none

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Interface configuration mode.

Mode

Usage Guide N/A

Configuration The following example disables **guard** on interface Gi 0/1.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree guard none
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

10.24 spanning-tree guard root

Use this command to enable **root guard** on the interface to prevent the change of current root bridge position because of error configuration and illegal packet attack. Use the **no** form of this command to restore the default setting.

spanning-tree guard root

no spanning-tree guard root

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide

- If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks.
- The loop guard function and root guard function cannot be enabled at the same time.

Configuration The following example enables **root guard** on the interface.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree guard root
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.25 spanning-tree ignore tc

Use this command to enable the tc filtering on the interface. Use the **no** form of this command to restore the default setting. With tc filtering enabled, the TC packets received on the interface will not be processed.

spanning-tree ignore tc

no spanning-tree ignore tc

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults This function is disabled by default.

Command Interface configuration mode.

Mode

Usage Guide If TC filter is enabled on a port, the port does not process received TC packets.

Configuration The following example enables the tc filtering on the interface.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-interface-id)# spanning-tree ignore tc
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

10.26 spanning-tree link-type

Use this command to configure the link type of the interface. Use the **no** form of this command to restore the default setting.

spanning-tree link-type [point-to-point | shared]

no spanning-tree link-type

**Parameter
Description**

Parameter	Description
point-to-point	Sets the link type of the interface to point-to-point.
shared	Forcibly sets the link type of the interface to shared.

Defaults For a full-duplex interface, its link type is set to point-to-point link; for a half-duplex interface, its link type is set to shared.

Command Interface configuration mode.

Mode

Usage Guide If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

Configuration The following example configures the link type of the interface.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id)# spanning-tree link-type point-to-point
```

Related Commands	Command	Description
		show spanning-tree interface

Platform N/A
Description

10.27 spanning-tree loopguard default

Use this command to enable **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the **no** form of this command to restore the default setting.

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter Description	Parameter	Description
		N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

Configuration Examples The following example enables **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpdu.

```
Ruijie(config)# spanning-tree loopguard default
```

Related Commands	Command	Description
		N/A

Platform N/A
Description

10.28 spanning-tree max-hops

Use this command to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode, the number of hops in a region that the BPDU message passes before

being dropped. This parameter takes effect for all instances. Use the **no** form of this command to restore the default setting.

spanning-tree max-hops *hop-count*

no spanning-tree max-hops

Parameter Description	Parameter	Description
	<i>hop-count</i>	Number of hops in a region that the BPDU message passes before being dropped. The range is 1 to 40 hops.

Defaults The default is 20 hops.

Command Mode Global configuration mode.

Usage Guide In the region, the BPDU message sent by the root bridge includes a Hop Count field. When the BPDU message passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates the BPDU message times out. The device will drop the BPDU message whose Hop Count is 0. Changing the max-hops command affects all instances.

Configuration Examples This example sets the max-hops of the spanning tree to 10 for all instances.

```
Ruijie(config)# spanning-tree max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** command in the privileged EXEC mode.

Related Commands	Command	Description
	show spanning-tree	Displays the MSTP information.

Platform Description N/A

10.29 spanning-tree mode

Use this command to set the STP version. Use the **no** form of the command to restore the default setting.

spanning-tree mode [*stp* | *rstp* | *mstp*]

no spanning-tree mode

Parameter Description	Parameter	Description
	<i>stp</i>	Spanning tree protocol(IEEE 802.1d)
	<i>rstp</i>	Rapid spanning tree protocol(IEEE 802.1w)
	<i>mstp</i>	Multiple spanning tree protocol(IEEE 802.1s)

Defaults The default is **mstp**.

Command

Mode Global configuration mode.

Usage Guide However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with Ruijie devices, run this command to switch the STP mode to a lower version.

Configuration The following example sets the STP version.

Examples

```
Ruijie(config)# spanning-tree mode stp
```

**Related
Commands**

Command	Description
show spanning-tree	Displays the spanning-tree configuration.

Platform N/A

Description

10.30 spanning-tree mst configuration

Use this command to enter the MST configuration mode in the global configuration mode and configure the MSTP region. Use the **no** form of the command to restore the default setting.

spanning-tree mst configuration

no spanning-tree mst configuration

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

Command Global configuration mode.

Mode

Usage Guide To return to the privileged EXEC mode, enter end or Ctrl+C.

To return to the global configuration mode, enter exit.

After entering the MST configuration mode, you can configure MSTP Region parameters:

Configuration This example enters the MST configuration mode.

Examples

```
Ruijie(config)# spanning-tree mst configuration
```

```

Ruijie(config-mst)# instance 1 vlan 3, 5-10
Ruijie(config-mst)# name region 1
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      : region1
Revision : 1Instance  Vlans Mapped
-----
0         1-2,4,11-4094
1         3,5-10
-----
Ruijie(config-mst)# exit
Ruijie(config)#

```

Related Commands

Command	Description
show spanning-tree mst	Displays the MST region configuration.
instance <i>instance-id</i> vlan <i>vlan-range</i>	Adds VLANs to the MST instance.
name	Configures the name of MST.
revision	Configures the version of MST.

Platform N/A

Description

10.31 spanning-tree mst cost

Use this command to set the path cost of an instance in the interface configuration mode. Use the **no** form of the command to restore the default setting.

spanning-tree [**mst** *instance-id*] **cost** *cost*

no spanning-tree [**mst** *instance-id*] *cost*

Parameter Description

Parameter	Description
instance-id	Instance ID in the range from 0 to 64.
cost	Path cost in the range from 1 to 200,000,000.

Defaults

The default instance-id is 0.

The default value is calculated by the link rate of the interface automatically.

1000 Mbps—20000

100 Mbps—200000

10 Mbps—2000000

Command

Interface configuration mode.

Mode

Usage Guide A higher cost value means a higher path cost.

Configuration This example sets the path cost to 400 on the interface associated with instances 3.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# spanning-tree mst 3 cost 400
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* command in the privileged EXEC mode.

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst port-priority	Configures the priority of an interface.
spanning-tree mst priority	Configures the priority of an instance.

Platform N/A

Description

10.32 spanning-tree mst port-priority

Use this command to configure the interface priority for different instances in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. Use the **no** form of this command to restore the default setting.

spanning-tree [mst *instance-id*] port-priority *priority*

no spanning-tree [mst *instance-id*] port-priority

Parameter Description

Parameter	Description
<i>Instance-id</i>	Instance ID, in the range of 0 to 64
<i>priority</i>	Interface priority. Sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, which are the multiples of 16.

Defaults The default instance-id is 0.
The default priority is 128.

Command Mode Interface configuration mode.

Usage Guide When a loop occurs in the region, the interface of the higher priority will be in charge of forwarding. If all interfaces have the same priority value, the interface of the smaller number will be in charge of the forwarding.
Run this command to determine which port in the loop of a region enters the forwarding state.

Configuration This example sets the priority of **gigabitethernet 1/1** to 10 in instance 20.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
```

Ruijie(config-if-interface-id)# spanning-tree mst 20 port-priority 0
You can verify your settings by entering the **show spanning-tree mst instance-id** privileged command.

Related Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst cost	Sets the path cost.
spanning-tree mst priority	Sets the device priority for different instances.

Platform N/A

Description

10.33 spanning-tree mst priority

Use this command to set the device priority for different instances in the global configuration mode.

Use the **no** form of this command to restore the default setting.

spanning-tree [mst instance-id] priority priority

no spanning-tree [mst instance-id] priority

Parameter Description

Parameter	Description
<i>instance-id</i>	Instance ID, in the range of 0 to 64
<i>priority</i>	Device priority. Sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440, which are all multiples of 4096.

Defaults

The default instance ID is 0.

The default device priority is 32768.

Command Mode

Global configuration mode.

Usage Guide

Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

Configuration

The following example sets the device priority of the Instance to 8192.

Examples

```
Ruijie(config)# spanning-tree mst 20 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst instance interface instance-id** command in the privileged EXEC mode.

Related Commands

Command	Description
---------	-------------

show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst cost	Sets path cost.
spanning-tree mst port-priority	Sets the port priority of an instance.

Platform N/A

Description

10.34 spanning-tree pathcost method

Use this command to configure the path cost of the port. Use the **no** form of this command to restore the default setting.

spanning-tree pathcost method { **long** [**standard**] | **short** }

no spanning-tree pathcost method

Parameter Description	Parameter	Description
	Long [standard]	Adopts the 802.1t standard to configure path cost. The standard indicates that use the expression recommended by the standard to calculate the cost value.
	short	Adopts the 802.1d standard to configure path cost.

Defaults 802.1T standard is adopted to set path cost by default.

Command Global configuration mode.

Mode

Usage Guide If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

Configuration The following example configures the path cost of the port.

Examples

```
Ruijie(config-if)# spanning-tree pathcost method long
```

Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.

Platform N/A

Description

10.35 spanning-tree portfast

Use this command to enable the portfast on the interface. Use the disabled form of this command to restore the default setting,

spanning-tree portfast [disabled]

Parameter Description	Parameter	Description
		disabled

Defaults This function is disabled by default.

Command Interface configuration mode.

Mode

Usage Guide After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.

Configuration The following example enables the portfast on the interface.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id)# spanning-tree portfast
```

Related Commands	Command	Description
		show spanning-tree interface

Platform N/A

Description

10.36 spanning-tree portfast bpdudfilter default

Use this command to enable the BPDU filter function globally. You can use the **no** form of the command to restore the default setting.

spanning-tree portfast bpdudfilter default

no spanning-tree portfast bpdudfilter default

Parameter Description	Parameter	Description
		N/A

Defaults This function is disabled by default,

Command Global configuration mode.

Mode

Usage Guide Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the interface. Use the **show spanning-tree** command to display the configuration.

Configuration The following example enables the BPDU filter function globally.

Examples

```
Ruijie(config)# spanning-tree portfast bpdupfilter default
```

**Related
Commands**

Command	Description
show spanning-tree interface	Displays the global STP configuration.

Platform N/A

Description

10.37 spanning-tree portfast bpduguard default

Use this command to enable the BPDU guard globally. Use the **no** form of this command to restore the default setting,

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

**Parameter
Description**


Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode.

Mode

Usage Guide Once the BPDU guard is enabled on the interface, it will enter the error-disabled status if the BPDU message arrives at the interface. Use the **show spanning-tree** command to display the configuration.

 The global BPDU guard takes effect only when PortFast is enabled on a port.

Configuration The following example enables the GPDU guard globally.

Examples

```
Ruijie(config)# spanning-tree portfast bpduguard  
default
```

**Related
Commands**

Command	Description
show spanning-tree interface	Displays the global STP configuration.

Platform N/A

Description

10.38 spanning-tree portfast default

Use this command to enable the portfast feature on all interfaces globally. Use the **no** form of this command to restore the default setting.

spanning-tree portfast default

no spanning-tree portfast default

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the portfast feature on all interfaces globally.

```
Ruijie(config)# spanning-tree portfast default
```

Related Commands	Command	Description
	show spanning-tree interface	Displays the global STP configuration.

Platform Description N/A

10.39 spanning-tree reset

Use this command to restore the **spanning-tree** configuration to the default setting.

spanning-tree reset

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode.

Usage Guide Enable TC guard to prevent TC packets from spreading.

Configuration The following example enables **tc-guard** on interface Gi 1/1.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-interface-id)# spanning-tree tc-guard
```

**Related
Commands**

Command	Description
show spanning-tree	Displays the global STP configuration.
show spanning-tree interface	Displays the STP configuration of the interface.

Platform N/A

Description

10.40 spanning-tree tc-guard

Use this command to enable **tc-guard** on the interface to prevent the spread of TC messages. Use the **no** form of this command to disable this function on the interface.

spanning-tree tc-guard

no spanning-tree tc-guard

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode.

Mode

Usage Guide N/A

Configuration The following example enables **tc-guard** on the interface to prevent the spread of TC messages.

Examples

```
Ruijie(config)# spanning-tree tc-guard
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

10.41 spanning-tree tc-protection

Use this command to enable **tc-protection** globally. Use The **no** form of this command to disable this function.

spanning-tree tc- protection

no spanning-tree tc- protection

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables **tc-protection** globally.

```
Ruijie(config)# spanning-tree tc-protection
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.42 spanning-tree tc-protection tc-guard

Use this command to enable tc-guard to prevent TC packets from being flooded. Use the **no** form of this command to restore the default setting.

spanning-tree tc-protection tc-guard

no spanning-tree tc-protection tc-guard

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Enable TC guard to prevent TC packets from spreading.

Configuration The following example enables tc-guard to prevent TC packets from being flooded.

Examples

```
Ruijie(config)# spanning-tree tc-protection tc-guard
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

10.43 spanning-tree tx-hold-count

Use this command to configure the TxHoldCount of the STP, the maximum number of the BPDU messages sent in one second. Use the **no** form of this command to restore the default setting.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

**Parameter
Description**

Parameter	Description
<i>tx-hold-count</i>	Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.

Defaults The default is 3.

**Command
Mode** Global configuration mode.

Usage Guide N/A

Configuration The following example sets the maximum number of the BPDU messages sent in one second.

Examples

```
Ruijie(config)# spanning-tree tx-hold-count 5
```

**Related
Commands**

Command	Description
show spanning-tree	Displays the global MSTP configuration.

**Platform
Description** N/A

11 GVRP Commands

11.1 bridge-frame forwarding protocol gvrp

Use this command to enable GVRP PDUs transparent transmission. Use the **no** form of this command to restore the default setting.

bridge-frame forwarding protocol gvrp

no bridge-frame forwarding protocol gvrp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide In the IEEE 802.1Q standard, the MAC address 01-80-C2-00-00-21 of GVRP PDUs is reserved for future standardization. In other words, the device following the IEEE 802.1Q standard does not forward GVRP PDUs frames. However, in actual network deployment, GVRP PDUs transparent transmission may be required. For example, the device not enabled with GVRP needs to transmit GVRP PDUs frames transparently to ensure proper GVRP topology calculation.

Configuration The following example enables GVRP PDUs transparent transmission.

Examples

```
Ruijie(config)# bridge-frame forwarding protocol gvrp
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

11.2 clear gvrp statistic

Use this command to clear the GVRP statistics for re-counting.

clear gvrp statistics { *interface-id* | **all** }

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>interface-id</i>	Interface id
---------------------	--------------

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide Use the **show gvrp statistics** to display the statistics.

Configuration The following example clears GVRP statistics.

Examples Ruijie# clear gvrp statistics all

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

11.3 gvrp applicant state

Use this command configures the GVRP advertisement mode on the interface.. Use the **no** form of this command to restore default setting.

gvrp applicant state { normal | non-applicant }

no gvrp applicant state

Parameter Description	Parameter	Description
	normal	The interface sends VLAN advertisement.
non-applicant	The interface does not send VLAN advertisement.	

Defaults The interface sends GVRP advertisement by default.

Command mode Interface configuration mode.

Usage Guide N/A

Configuration The following example configures the GVRP advertisement mode on the interface.

Examples Ruijie(config-if)# gvrp applicant state normal

Related Commands	Command	Description

show gvrp configuration	Displays the GVRP configurations.
-------------------------	-----------------------------------

Platform N/A

Description

11.4 gvrp dynamic-vlan-creation

Use this command to enable dynamic VLAN creation. Use the **no** form of this command to restore the default setting.

gvrp dynamic-vlan-creation enable

no gvrp dynamic-vlan-creation enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Global configuration mode.

Usage Guide Use the **show gvrp configuration** to display the configuration.

Configuration The following example enables dynamic VLAN creation.

Examples

```
Ruijie(config)# gvrp dynamic-vlan-creation enable
```

Related Commands	Command	Description
	show gvrp configuration	Displays the GVRP configurations.

Platform N/A

Description

11.5 gvrp enable

Use this command to enable the GVRP function. Use the **no** form of this command to restore the default setting.

gvrp enable

no gvrp enable

Parameter Description	Parameter	Description
	N/A	N/A

- Defaults** This function is disabled by default.
- Command mode** Global configuration mode
- Usage Guide** This command is used to display the configuration.

Configuration The following example enables the GVRP function.

Examples

```
Ruijie(config)#gvrp enable
```

Related Commands	Command	Description
		show gvrp configuration

Platform N/A

Description

11.6 gvrp registration mode

Use this command to set the registration mode to control whether to enable dynamic VLAN creation/registration/canceling on the port. Use the **no** form of this command to restore the default setting.

gvrp registration mode { normal | disabled }

no gvrp registration mode

Parameter Description	Parameter	Description
		normal
	disabled	Disables dynamic VLAN creation/registration/canceling on the port.

Defaults Dynamic VLAN creation/registration/canceling is enabled by default,

Command mode Interface configuration mode.

Usage Guide N/A

Configuration The following example sets the registration mode.

Examples

```
Ruijie(config-if)# gvrp registration mode normal
```

Related Commands	Command	Description
		show gvrp configuration

Platform N/A
Description

11.7 gvrp timer

Use this command to set the GVRP timer. Use the **no** form of this command to restore the default setting.

gvrp timer { **join** *timer_value* | **leave** *timer_value* | **leaveall** *timer_value* }
no gvrp timer

Parameter Description

Parameter	Description
<i>join timer_value</i>	Controls the maximum delay before sending the advertisement on the port. The actual sending interval is in the range of 0 to the maximum delay.
<i>leave timer_value</i>	Controls the waiting time before removing the VLAN from the port with the Leave Message received. If the Join Message is received again within this time range, the port-VLAN relation still exists and the timer becomes invalid. If no Join Message is received on the port, the port status will be the Empty and removed from the VLAN member list.
<i>leave all timer_value</i>	Controls the minimum interval of sending the LeaveAll Message on the port. If the LeaveAll Message is received before the timer expires, the timer re-counts. If the timer expires, send the LeaveAll Message on the port and also send this Message to the port, so that the Leave timer begins counting. The actual sending interval ranges from <i>leaveall</i> to <i>leaveall+join</i> .

Defaults Join timer: 200 milliseconds;
 Leave timer: 600 milliseconds;
 Leaveall timer: 10000 milliseconds.

Command mode Global configuration mode

Usage Guide Use the **show gvrp configuration** to display the configuration.
 Use the **no gvrp timer** command to restore **join**, **leave** and **leaveall timer** to default settings.

Configuration The following example configures the join timer.

Examples Ruijie(config)# gvrp timer join 200

Related Commands

Command	Description
---------	-------------

show gvrp configuration	Displays the GVRP configuration.
-------------------------	----------------------------------

Platform N/A

Description

11.8 l2protocol-tunnel gvrp

Use this command to enable global GVRP PDUs TUNNEL globally. Use the **no** form of this command to restore the default setting.

l2protocol-tunnel gvrp

no l2protocol-tunnel gvrp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide If you want to enable global GVRP PDUs TUNNEL, enable GVRP PDUs TUNNEL on the interface first.

Configuration The following example enables GVRP PDUs TUNNEL globally.

Examples

```
Ruijie(config)# l2protocol-tunnel gvrp
Ruijie(config)# show l2protocol-tunnel gvrp

L2protocol-tunnel: Gvrp Disable
L2protocol-tunnel destination mac address:01d0.f800.0006
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

11.9 l2protocol-tunnel gvrp enable

Use this command to enable GVRP PDUs TUNNEL on the interface. Use this command to restore the default setting.

l2protocol-tunnel gvrp enable

no l2protocol-tunnel gvrp enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Interface configuration mode

Usage Guide If you want to enable global GVRP PDUs TUNNEL, enable GVRP PDUs TUNNEL on the interface first.

Configuration The following example enables GVRP PDUs TUNNEL on the interface.

Examples

```
Ruijie(config-if-interface-id)# l2protocol-tunnel gvrp enable
Ruijie(config-if-interface-id)# show l2protocol-tunnel gvrp

L2protocol-tunnel: Gvrp Disable
L2protocol-tunnel destination mac address:01d0.f800.0006
GigabitEthernet 0/1 l2protocol-tunnel gvrp enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

11.10 l2protocol-tunnel gvrp tunnel-dmac

Use this command to configure the MAC address for transparent transmission in GVRP PDUs TUNNEL. Use the **no** form of this command to restore the default setting.

l2protocol-tunnel gvrp tunnel-dmac *mac-address*

no l2protocol-tunnel gvrp tunnel-dmac

Parameter Description	Parameter	Description
	<i>mac-address</i>	The MAC address for transparent transmission in GVRP PDUs TUNNEL.

Defaults The default is 01d0.f800.0006.

Command Global configuration mode

mode

Usage Guide The available MAC address f ranges from 01d0.f800.0006 to 011a.a900.0006.

Configuration The following example configures the MAC address for transparent transmission in GVRP PDUs

Examples TUNNEL.

```
Ruijie(config)# l2protocol-tunnel gvrp tunnel-dmac 011a.a900.0006
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

11.11 show gvrp configuration

Use this command to display the GVRP configuration.

show gvrp configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide Use the **show gvrp configuration** to display the configuration.

Configuration The following example displays GVRP configuration.

Examples

```
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Leave Timers(ms):600
Leaveall Timers(ms):1000
Port based GVRP Configuration:
      PORT                Applicant Status          Registration Mode
-----
GigabitEthernet 0/2          normal                normal
```

Field	Description
GVRP Feature	Whether to enable GVRP

GVRP dynamic VLAN creation	Whether to enable dynamic VLAN creation
Join Timers	Join timer
Leave Timers	Leave timer
Leaveall Timers	Leaveall timer
PORT	Port
Applicant Status	Advertisement mode
Registration Mode	Registration mode

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

11.12 show gvrp statistics

Use this command to display the GVRP statistics of one interface or all interfaces.

show gvrp statistics { *interface-id* | **all** }

**Parameter
Description**

Parameter	Description
<i>interface-id</i>	Interface id.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use the **show gvrp statistics** to display the statistics of one interface or all interfaces.

Configuration Ruijie# show gvrp statistics gigabitethernet 1/1

Examples Interface GigabitEthernet 3/1

```

RecValidGvrpPdu      0
RecInvalidGvrpPdu    0
RecJoinEmpty         0
RecJoinIn            0
RecEmpty             0
RecLeaveEmpty         0
RecLeaveIn            0
RecLeaveAll           0
SentGvrpPdu          0
SentJoinEmpty        0

```

```

SentJoinIn      0
SentEmpty       0
SentLeaveEmpty   0
SentLeaveIn      0
SentLeaveAll     0
JoinIndicated   0
LeaveIndicated   0
JoinPropagated  0
LeavePropagated  0

```

Field	Description
RecValidGvrpPdu	Number of received valid GPDU packets.
RecInvalidGvrpPdu	Number of received invalid GPDU packets.
RecJoinEmpty/ SentJoinEmpty	Number of received/sent JoinEmpty messages.
RecJoinIn/ SentJoinIn	Number of received/sent JoinIn messages.
RecEmpty/SentEmpty	Number of received/sent Empty messages.
RecLeaveEmpty/SentLeaveEmpty	Number of received/sent LeaveEmpty messages,
RecLeaveIn/ SentLeaveIn	Number of received/sent LeaveIn messages.
RecLeaveAll/SentLeaveAll	Number of received/sent LeaveAll messages.
SentGvrpPdu	Number of sent GPDU messages.
JoinIndicated/ LeaveIndicated	Number of Join/Leave service requests.
JoinPropagated / LeavePropagated	Number of Join/Leave topology update requests.

Related Commands

Command	Description
clear gvrp statistics	Clears the statistics of one interface or all interfaces.

Platform N/A

Description

11.13 show gvrp status

Use this command to display all dynamic VLAN ports generated by GVRP and the dynamic VLAN ports added to the static VLAN.

show gvrp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide Use the **show gvrp status** command to display the GVRP status.

Configuration The following example displays the GVRP status.

Examples

```
Ruijie# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 2
Dynamic Ports:
```

Field	Description
VLAN	Static VLAN
DVLAN	Dynamic VLAN
Dynamic Ports	Dynamic ports.

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

11.14 show l2protocol-tunnel gvrp

Use this command to display GVRP PDUs TUNNEL configuration.

show l2protocol-tunnel gvrp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays GVRP PDUs TUNNEL configuration.

Examples

```
Ruijie# show l2protocol-tunnel gvrp
```

```
L2protocol-tunnel: Gvrp Enable
L2protocol-tunnel destination mac address:011a.a900.0006
GigabitEthernet 0/1 l2protocol-tunnel gvrp enable
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

12 LLDP Commands

12.1 { voice | voice-signaling } vlan

Use this command to configure the LLDP network policy. Use the **no** form of this command to delete the policy.

```
{ voice | voice-signaling } vlan { { vlan-id [ cos cvalue | dscp dvalue ] } | { dot1p [ cos cvalue | dscp dvalue ] } | none | untagged }
```

```
no { voice | voice-signaling } vlan
```

Parameter	Parameter	Description
Description	voice	Voice application
	voice-signaling	Voice-signaling application
	<i>vlan-id</i>	(Optional) VLAN ID of voice flow. The value ranges from 1 to 4094.
	cos	(Optional) Class of service
	<i>cvalue</i>	(Optional) CoS of the configured voice flow. The value ranges from 0 to 7, and the default value is 5.
	dscp	(Optional) Differentiated services code point
	<i>dvalue</i>	(Optional) DSCP value of the configured voice flow. The value ranges from 0 to 63. The default value is 46.
	dot1p	(Optional) 802.1p priority tagging. The tag frame includes user_priority and vlan id is 0.
	none	(Optional) The network policy is not advertised. VoIP determines the network policy based on its configuration.
	untagged	(Optional) The untag frame is sent in the voice vlan in VoIP. In this case, the value of vlan id and cos are ignored.

Defaults N/A

Command LLDP network policy configuration mode

Mode

Usage Guide In the LLDP network policy configuration mode, configure the LLDP network policy.

Configuration Examples The following example configures the LLDP network policy (profile-num is 1).

```
Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan untagged
Ruijie(config-lldp-network-policy)# voice-signaling vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice-signaling vlan 3 dscp 6
```


Related	Command	Description
Commands	show lldp network-policy profile [<i>profile-num</i>]	Displays the LLDP network policy.

Platform N/A

Description

12.2 civic-location

Use this command to configure a common LLDP address. Use the **no** form of this command to delete the address.

civic-location { **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*

no civic-location { **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*

Parameter	Parameter	Description
Description	country	Country code, two bytes. For example, the country code of China is CH.
	state	Address information, CA type 1
	county	CA type 2
	city	CA type 3
	division	CA type 4
	neighborhood	CA type 5
	street-group	CA type 6
	leading-street-dir	CA type 16
	trailing-street-suffix	CA type 17
	street-suffix	CA type 18
	number	CA type 19
	street-number-suffix	CA type 20
	landmark	CA type 21
	additional-location-information	CA type 22
	name	CA type 23
	postal-code	CA type 24
	building	CA type 25
unit	CA type 26	
floor	CA type 27	

room	CA type 28
type-of-place	CA type 29
postal-community-name	CA type 30
post-office-box	CA type 31
additional-code	CA type 32
<i>ca-word</i>	Address information

Defaults N/A

Command LLDP Civic address configuration mode

Mode

Usage Guide This command is used to configure a common LLDP address in LLDP Civic address configuration mode.

Configuration The following example configures an LLDP Civic Address (ID: 1).

Examples

```
Ruijie#config
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
```

Related	Command	Description
Commands	show lldp location civic-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays the information about an LLDP Civic address.

Platform N/A

Description

12.3 clear lldp statistics

Use this command to clear LLDP statistics.

clear lldp statistics [interface *interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide **interface** parameter: clear the LLDP statistics of the specified interface

Configuration The following example clears LLDP statistics of interface 1.

Examples

```
Ruijie# clear lldp statistics interface GigabitEthernet 0/1
Ruijie# show lldp statistics interface GigabitEthernet 0/1
Lldp statistics information of port [GigabitEthernet 0/1]
-----
The number of lldp frames transmitted : 0
The number of frames discarded      : 0
The number of error frames          : 0
The number of lldp frames received  : 0
The number of TLVs discarded        : 0
The number of TLVs unrecognized     : 0
The number of neighbor information aged out : 0
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

12.4 clear lldp table

Use this command to clear LLDP neighbor information.

clear lldp table [**interface** *interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the **interface** parameter is specified, the LLDP neighbor information on the specified interface is cleared.
If the **interface** parameter is not specified, the LLDP neighbor information on all interfaces is cleared.

Configuration The following example clears the LLDP neighbor information on interface 1.

Examples

```
Ruijie# show lldp neighbors interface GigabitEthernet 0/1
Lldp statistics information of port [GigabitEthernet 0/1]
-----
The number of lldp frames transmitted : 0
The number of frames discarded      : 0
The number of error frames          : 0
The number of lldp frames received  : 0
```

```

The number of TLVs discarded      : 0
The number of TLVs unrecognized   : 0
The number of neighbor information aged out : 0
Ruijie# clear lldp table interface GigabitEthernet 0/1
Ruijie# show lldp neighbors interface GigabitEthernet 0/1

```

Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

12.5 device-type

Use this command to configure the device type. Use the **no** form of this command to restore the default setting.

device-type *device-type*

no device-type

Parameter	Parameter	Description
Description	<i>device-type</i>	Device type. The value ranges from 0 to 2. 0: The device type is DHCP Server. 1: The device type is switch. 2: The device type is LLDP MED terminal.

Defaults The default is 1.

Command Mode LLDP Civic address configuration mode

Usage Guide This command is used to configure the device type in a common LLDP address in LLDP Civic address configuration mode.

Configuration Examples The following example sets the device type to switch.

```

Ruijie#config
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# device-type 1

```

Related Commands	Command	Description
	show lldp location civic-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays LLDP Civic Address information.

Platform N/A

Description

12.6 lldp compliance vendor

Use this command to enable detection of compatible neighbors.

lldp compliance vendor

no lldp compliance vendor

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables detection of compatible neighbors.	
	<pre>Ruijie#configure terminal Ruijie(config)# lldp compliance vendor</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

12.7 lldp enable

Use this command to enable the LLDP globally or on the interface. Use **no** form of this command to disable this function.

lldp enable

no lldp enable

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global (or interface) configuration mode	
Usage Guide	LLDP takes effect on an interface only when LLDP is enabled globally.	

Configuration The following example disables LLDP globally and on the interface.

Examples

```
Ruijie#config
Ruijie(config)#no lldp enable
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)# no lldp enable
```

Related	Command	Description
Commands	show lldp status	Displays LLDP status information.

Platform N/A

Description

12.8 lldp encapsulation snap

Use this command to configure the encapsulation format of LLDP packets. Use the **no** form of this command to restore the default setting.

lldp encapsulation snap

no lldp encapsulation snap

Parameter	Parameter	Description
Description	N/A	N/A

Defaults By default, Ethernet II encapsulation format is used.

Command Interface configuration mode.

Mode

Usage Guide



Caution To guarantee the normal communication between local device and neighbor device, the same LLDP packet encapsulation format must be used.

Configuration The following example sets LLDP packet encapsulation format to

Examples

```
SNAP.Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp encapsulation snap
```

Related	Command	Description
Commands	show lldp status	Displays LLDP status information.

Platform N/A
Description

12.9 lldp error-detect

Use this command to configure the LLDP error detection, including the detection of VLAN configurations on both sides of the link, port state detection, port aggregation configuration detection, MTU configuration detection and loop detection. If any error is detected by LLDP, warning message will be printed to notify the administrator. Use the **no** form of this command to disable this function.

lldp error-detect
no lldp error-detect

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Interface configuration mode.
Mode

Usage Guide LLDP error detection relies on the specific TLV in the LLDP packets exchanged between devices on both sides of the link. To ensure normal functioning of the detection feature, correct TLVs must be advertised.

Configuration The following example configures LLDP error detection.

Examples

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp error-detect
```

Related	Command	Description
Commands	show interface status	Displays LLDP status information.

Platform N/A
Description

12.10 lldp fast-count

When a new neighbor is detected or when LLDP operating mode changes from shutdown or Rx to TxRx or Tx, to allow the neighbor device to quickly study the information about this device, the fast sending mechanism will be initiated. The fast sending mechanism shortens the LLDPDU sending interval to 1 second and continuously transmits a certain number of LLDPDUs before restoring to the normal transmit interval. Use the **no** form of this command to restore the default setting.

lldp fast-count *value*

no lldp fast-count

Parameter	Parameter	Description
Description	<i>value</i>	The number of fast sent LLDP packets, in the range from 1 to 10.
Defaults	The default is 3.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the number of fast sent LLDP packets to 5.	
	<pre>Ruijie#config Ruijie(config)#lldp fast-count 5</pre>	
Related Commands	Command	Description
	show interface status	Displays LLDP status information.
Platform Description	N/A	

12.11 lldp hold-multiplier

Use this command to set the TTL multiplier. Use the **no** form of this command to restore to default setting.

lldp hold-multiplier *value*

no lldp hold-multiplier

Parameter	Parameter	Description
Description	<i>value</i>	TTL multiplier, in the range from 2 to 10.
Defaults	The default is 4.	
Command Mode	Global configuration mode.	
Usage Guide	The value of Time To Live (TLV) in LLDP packet = TTL multiplier × LLDP packet transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.	
Configuration Examples	The following example sets TTL multiplier to 5.	
	<pre>Ruijie#config Ruijie(config)#lldp hold-multiplier 5</pre>	

Related	Command	Description
Commands	show lldp status	Displays LLDP status information.

Platform N/A

Description

12.12 lldp location civic-location identifier

Use this command to create a common address of a device connected to the network in LLDP Civic Address configuration mode. Use the **no** form of this command to delete the address.

lldp location civic-location identifier *id*

no lldp location civic-location identifier *id*

Parameter	Parameter	Description
Description	<i>id</i>	ID of a common address of a network device, in the range from 1 to 1024.

Defaults N/A

Command Global configuration mode
Mode

Usage Guide This command can be used to enter the LLDP Civic Address configuration mode.

Configuration Examples The following example creates the Civic Address information in LLDP MED-TLV as follows: set *id* to 1.

```
Ruijie#config
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)#
```

Related	Command	Description
Commands	show lldp location civic-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays the LLDP Civic Address information.

Platform N/A

Description

12.13 lldp location elin identifier

Use this command to set an emergency number encapsulated in a Location Identification TLV. Use the **no** form of this command to delete the number.

lldp location elin identifier *id elin-location tel-number*

no lldp location elin identifier *id*

Parameter	Parameter	Description
Description	<i>id</i>	ID of an emergency number, in the range from 1 to 1024.
	<i>tel-number</i>	Emergency number, in the range from 10 to 25 bytes.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure an emergency number.

Configuration The following example sets an emergency number.

Examples

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
```

Related Commands	Command	Description
	show lldp location elin-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays an LLDP emergency number.

Platform N/A

Description

12.14 lldp management-address-tlv

Use this command to configure the management address advertised in LLDP packets. Use the **no** form of this command to disable the advertisement of management address.

lldp management-address-tlv [*ip-address*]

no lldp management-address-tlv

Parameter	Parameter	Description
Description	<i>ip-address</i>	The management address advertised in LLDP packets.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide By default, the management address is advertised in LLDP packets, and is the IPv4 address of the lowest-ID VLAN carried on the port. If IPv4 address is not configured for this VLAN, the next lowest-ID VLAN carried on the port will be tried until the IPv4 address is obtained.

If the IPv4 address is still not found, the IPv6 address of the lowest-ID VLAN carried on the port will be tried.

If the IPv6 address is still not found, the MAC address of the device will be advertised as the management address.

Configuration Examples The following example configures the management address advertised in LLDP packets to 192.168.1.1.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp management-address-tlv 192.168.1.1
```

Related Commands	Command	Description
	show lldp local-information	Displays LLDP local information

Platform N/A
Description

12.15 lldp mode

Use this command to configure the LLDP operating mode. Use **no** form of this command to restore the default setting.

lldp mode { rx | tx | txrx }

no lldp mode

Parameter Description	Parameter	Description
	rx	Only sends LLDPDUs.
	tx	Only receives LLDPDUs.
	txrx	Sends and receives LLDPDUs.

Defaults The default is **txrx**.

Command Mode Interface configuration mode

Usage Guide Disable LLDP operating mode on the interface. The interface won't send and receive LLDP packets. The precondition for enabling LLDP on the interface is that LLDP has been enabled globally and LLDP operates in tx, rx or txrx mode.

Configuration Examples The following example sets LLDP operating mode to tx on the interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp mode tx
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information

Platform N/A

Description

12.16 lldp network-policy profile

Use this command to create an LLDP network policy and enter the LLDP network policy configuration mode. Use the **no** form of this command to delete the policy.

lldp network-policy profile *profile-num*

no lldp network-policy profile *profile-num*

Parameter	Parameter	Description
Description	<i>profile-num</i>	ID of an LLDP network policy, in the range from 1 to 1024.

Defaults N/A

Command Global configuration mode

Mode

Usage Guide This command is used to enter the LLDP network policy configuration mode. When this command is run, the policy ID must be specified.

In LLDP network-policy mode, the { **voice** | **voice-signaling** } **vlan** command can be used to configure the specific network policy.

Configuration Examples The following example creates an LLDP network policy whose ID is 1.

Examples

```
Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)#
```

Related Commands	Command	Description
	show lldp network-policy profile [<i>profile-num</i>]	Displays an LLDP network policy.

Platform N/A

Description

12.17 lldp notification remote-change enable

Use this command to configure LLDP Trap. Use the **no** form of this command to restore the default setting.

lldp notification remote-change enable

no lldp notification remote-change enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide By configuring LLDP Trap, the LLDP information of local device (such as information about the detection of new neighbor or the fault on the communication link) can be sent to the network management server. The administrator can monitor the network operation status according to such information.

Configuration Examples The following example configures LLDP Trap.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp notification remote-change enable
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform Description N/A

12.18 lldp timer notification-interval

Use this command to set an interval of sending LLDP Traps. Use the **no** form of this command to restore the default setting.

lldp timer notification-interval *seconds*

no lldp timer notification-interval

Parameter	Parameter	Description
Description	<i>seconds</i>	Interval of sending LLDP Traps, in the range from 5 to 3600 in the unit of seconds.

Defaults The default is 5.

Command Mode Global configuration mode.

Usage Guide To prevent excessive LLDP traps from being sent, you can set an interval of sending LLDP Traps. If LLDP information change is detected during this interval, traps will be sent to the network management server.

Configuration The following example sets the interval of sending LLDP Traps to 10 seconds.

Examples

```
Ruijie#config
Ruijie(config)#lldp timer notification-interval 10
```

Related	Command	Description
Commands	show lldp status	Displays LLDP status information.

Platform N/A

Description

12.19 lldp timer reinit-delay

Use this command to set port initialization delay. Use the **no** form of this command to restore the default setting.

lldp timer reinit-delay *seconds*

no lldp timer reinit-delay

Parameter	Parameter	Description
Description	<i>seconds</i>	Port initialization delay, in the range from 1 to 10 in the unit of seconds.

Defaults The default is 2.

Command Global configuration mode.

Mode

Usage Guide To prevent LLDP from being initialized too frequently due to the frequent operating mode change, you can configure port initialization delay.

Configuration The following example sets LLDP port initialization delay to 3 seconds.

Examples

```
Ruijie#config
Ruijie(config)#lldp timer reinit-delay 3
```

Related	Command	Description
Commands	show lldp status	Displays LLDP status information.

Platform N/A

Description

12.20 lldp timer tx-delay

Use this command to set LLDP packet transmission delay. Use the **no** form of this command to restore the default setting.

lldp timer tx-delay *seconds*

no lldp timer tx-delay

Parameter	Parameter	Description
Description	<i>seconds</i>	LLDP packet transmission delay, in the range from 1 to 8192 in the unit of seconds.

Defaults The default is 2.

Command Global configuration mode.

Mode

Usage Guide An LLDP-enabled port will send LLDP packets when the local device information changes. To avoid frequently sending LLDP packets due to the frequent local device information change, configure the LLDP packet transmission delay to control the frequent transmission of LLDP packets.

Configuration Examples The following example sets LLDPDU transmission delay to 3 seconds.

```
Ruijie#config
Ruijie(config)#lldp timer tx-delay 3
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform N/A

Description

12.21 lldp timer tx-interval

Use this command to set the interval of sending the LLDP packets. Use **no** form of this command to restore the default setting.

lldp timer tx-interval *seconds*

no lldp timer tx-interval

Parameter	Parameter	Description
Description	<i>seconds</i>	Interval of sending the LLDP packets, in the range from 5 to 32768 in the unit of seconds.

Defaults The default is 30.

Command Global configuration mode.

Mode

Usage Guide N/A

Configuration The following example sets the interval of sending the LLDP packets to 10 seconds.

Examples

```
Ruijie#config
Ruijie(config)#lldp timer tx-interval 10
```

Related	Command	Description
Commands	show lldp status	Displays LLDP status information.

Platform N/A

Description

12.22 lldp tlv-enable

Use this command to configure the types of advertisable TLVs. Use the **no** form of this command to restore the default setting.

```
lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description |
system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ] } |
dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability
| inventory | location { civic-location | elin } identifier id | network-policy profile [ profile-num ] |
power-over-ethernet } }
```

```
no lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description |
system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name } | dot3-tlv { all |
link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory |
location { civic-location | elin } identifier id | network-policy profile [ profile-num ] |
power-over-ethernet } }
```

Parameter	Parameter	Description
Description	basic-tlv	Basic management TLV
	port-description	Port Description TLV
	system-capability	System Capabilities TLV
	system-description	System Description TLV
	system-name	System Name TLV
	dot1-tlv	802.1 organizationally specific TLV
	port-vlan-id	Port VLAN ID TLV
	protocol-vlan-id	Port And Protocol VLAN ID TLV

<i>vlan-id</i>	VLAN ID
vlan-name	VLAN Name TLV
<i>vlan-id</i>	VLAN ID corresponding to the specified VLAN name
dot3-tlv	802.3 organizationally specific TLV
link-aggregation	Link Aggregation TLV
mac-physic	MAC/PHY Configuration/Status TLV
max-frame-size	Maximum Frame Size TLV
power	Power Via MDI TLV
med-tlv	LLDP MED TLV
capability	LLDP-MED Capabilities TLV
inventory	Inventory management TLVs, including hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.
location	Location Identification TLV
civic-location	Common address information about the network device in location identification TLVs.
elin	Encapsulated emergency number
<i>id</i>	Policy ID
network-policy	Network Policy TLV
<i>profile-num</i>	ID of network policy
power-over-ethernet	Extended Power-via-MDI TLV

Defaults By default, all TLVs other than Location Identification TLV can be advertised on the interface for products other than S12000. For the S12000 product series, only basic TLVs and IEEE 802.1 TLVs are advertised. To advertise IEEE 802.3 TLVs and LLDP-MED TLVs, run the **lldp tlv-enable** command.

Command Interface configuration mode
Mode

Usage Guide During configuration of basic management TLVs, IEEE 802.1 TLVs, and IEEE 802.3 TLVs, if the **all** parameter is specified, all optional TLVs of the types are advertised.
During configuration of LLDP-MED TLVs, if the **all** parameter is specified, all LLDP-MED TLVs except Location Identification TLVs are advertised.
When configuring LLDP-MED Capability TLVs, configure LLDP-MED MAC/PHY TLVs first. When canceling LLDP-MED MAC/PHY TLVs, cancel LLDP-MED Capability TLVs first.
When configuring LLDP-MED TLVs, configure LLDP-MED Capability TLVs first so that LLDP-MED TLVs of other types can be configured.
To cancel LLDP-MED TLVs, cancel LLDP-MED TLVs of other types first so that LLDP-MED Capability TLVs can be canceled.

Configuration The following example configures all IEEE 802.1 TLVs to be advertised.

Examples

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable dot1-tlv all
```

The following example applies LLDP network policy 1 on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv network-policy
profile 1
```

The following example applies the LLDP Civic Address (ID: 1) configuration on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv location
civic-location identifier 1
```

The following example applies the emergency number (ID: 1) on the 0/1 interface.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp location elin identifier 1
```

Related Commands	Command	Description
	show lldp tlv-config interface	Displays the attributes of advertisable TLVs

Platform N/A
Description

12.23 show lldp local-information

Use this command to display the LLDP information of local device. The information will be encapsulated in the TLVs and sent to the neighbor device.

show lldp local-information [**global** | **interface** *interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

- Usage Guide**
- **global** parameter: display the global LLDP information to be sent.
 - **Interface** parameter: displays the LLDP information to be sent out the interface specified.
 - No parameter: display all LLDP information, including global and interface-based LLDP

information.

Configuration The following example displays the device information to be sent to neighbor device.

Examples

```
Ruijie# show lldp local-information
Global LLDP local-information:
  Chassis ID type      : MAC address
  Chassis id          : 00d0.f822.33aa
  System name         : System name
  System description  : System description
  System capabilities supported : Repeater, Bridge, Router
  System capabilities enabled  : Repeater, Bridge, Router

  LLDP-MED capabilities  : LLDP-MED Capabilities, Network Policy, Location
    Identification, Extended Power via MDI-PD, Inventory
  Device class        : Network Connectivity
  HardwareRev         : 1.0
  FirmwareRev         :
  SoftwareRev         : RGOS 10.4(3) Release(94786)
  SerialNum           : 1234942570001
  Manufacturer name   : Manufacturer name
  Asset tracking identifier :

-----
Lldp local-information of port [GigabitEthernet 0/1]
-----

  Port ID type        : Interface name
  Port id             : GigabitEthernet 0/1
  Port description    :

  Management address subtype : 802 mac address
  Management address   : 00d0.f822.33aa
  Interface numbering subtype :
  Interface number     : 0
  Object identifier    :

  802.1 organizationally information
  Port VLAN ID        : 1
  Port and protocol VLAN ID (PPVID) : 1
  PPVID Supported     : YES
  PPVID Enabled       : NO
  VLAN name of VLAN 1 : VLAN0001
  Protocol Identity   :
```

```

802.3 organizationally information
Auto-negotiation supported : YES
Auto-negotiation enabled  : YES
PMD auto-negotiation advertised : 100BASE-TX full duplex mode, 100BASE-TX half
duplex mode
Operational MAU type      :
PoE support               : NO
Link aggregation supported : YES
Link aggregation enabled  : NO
Aggregation port ID      : 0
Maximum frame Size       : 1500

LLDP-MED organizationally information
Power-via-MDI device type : PD
Power-via-MDI power source : Local
Power-via-MDI power priority :
Power-via-MDI power value :
Model name                : Model name

```

show lldp local-information command output description:

Field	Description
Chassis ID type	Chassis ID type for identifying the Chassis ID field
Chassis ID	Used to identify the device, and is generally represented with MAC address
System name	Name of the sending device
System description	Description of the sending device, including hardware/software version, operating system and etc.
System capabilities supported	Capabilities supported by the system
System capabilities enabled	Capabilities currently enabled by the system
LLDP-MED capabilities	LLDP-MED capabilities supported by the system
Device class	MED device class, which is divided into 2 categories: network connectivity device and terminal device. Network connectivity device Class I: normal terminal device Class II: media terminal device; besides Class I capabilities, it also supports media streams. Class III: communication terminal device; it supports all the capabilities of Class I and Class II and IP communication.
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number

Manufacturer name	Device manufacturer
Asset tracking identifier	Asset tracking ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Management address subtype	Management address type
Management address	Management address
Interface numbering subtype	Type of the interface identified by the management address
Interface number	ID of the interface identified by the management address
Object identifier	ID of the object identified by the management address
Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID	Port and Protocol VLAN ID
PPVID Supported	Indicates whether port and protocol VLAN is supported
PPVID Enabled	Indicates whether port and protocol VLAN is enabled
VLAN name of VLAN 1	Name of VLAN 1
Protocol Identity	Protocol identifier
Auto-negotiation supported	Indicates whether auto-negotiation is supported
Auto-negotiation enabled	Indicates whether auto-negotiation is enabled
PMD auto-negotiation advertised	Auto-negotiation advertising capability of the port
Operational MAU type	Speed and duplex state of the port
PoE support	Indicates whether POE is supported
Link aggregation supported	Indicates whether link aggregation is supported
Link aggregation enabled	Indicates whether link aggregation is enabled
Aggregation port ID	ID of the link aggregation port
Maximum frame Size	Maximum frame size supported by the port
Power-via-MDI device type	Device type, including: PSE (power sourcing equipment) PD (powered device)
Power-via-MDI power source	Power source type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Available power on port
Model name	Name of model

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

12.24 show lldp location

Use this command to display the common LLDP address or emergency number of the local device.

show lldp location { **civic-location** | **elin** } { **identifier** *id* | **interface** *interface-name* | **static** }

Parameter	Parameter	Description
Description	civic-location	Encapsulates a common address of a network device.
	elin	Encapsulates an emergency number.
	identifier	Displays one address or emergency number configured.
	<i>id</i>	Policy ID of configured information
	interface	Displays the address or emergency number on an interface.
	<i>interface-name</i>	Interface name
	static	Displays all addresses or emergency numbers configured.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the policy ID is specified, the specified address or emergency number is displayed.
 If the interface name is specified, the address or emergency number configured on the interface is displayed.
 If no parameter is specified, all addresses or emergency numbers are displayed.

Configuration Examples The following example displays all addresses.

```
Ruijie# show lldp location civic-location static
LLDP Civic location information
-----
Identifier      : testt
County         : china
City Division   : 22
Leading street direction : 44
Street number   : 68
Landmark       : 233
Name           : liuy
Building       : 19bui
Floor          : 1
Room          : 33
City          : fuzhou
Country       : 86
Additional location : aaa
Ports         : Gi0/1
-----
Identifier      : tee
-----
```

The following example displays all emergency numbers.

```
Ruijie# show lldp location elin-location static
Elin location information
-----
Identifier : t
Elin      : iiiiixixixi
Ports     : Gi1/0/3
-----
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

12.25 show lldp neighbors

Use this command to display the LLDP information about a neighboring device.

show lldp neighbors [**interface** *interface-name*] [**detail**]

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
	detail	All information about a neighboring device

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the **detail** parameter is not specified, the brief information about a neighboring device is displayed. If the **detail** parameter is specified, the detailed information about a neighboring device is displayed. If the **interface** parameter is specified, the neighboring device information received on the specified interface is displayed.

Configuration Examples The following example displays the neighboring device information received on all ports.

```
Ruijie# show lldp neighbors detail
Lldp neighbor-information of port [GigabitEthernet 0/1]
Neighbor index      : 1
Device type         : LLDP Device
Update time         : 1hour 53minutes 30seconds
Aging time          : 5seconds
```

```
Chassis ID type      : MAC address
Chassis id          : 00d0.f822.33cd
System name         : System name
System description  : System description
System capabilities supported : Repeater, Bridge, Router
System capabilities enabled : Repeater, Bridge, Router

Management address subtype : 802 mac address
Management address   : 00d0.f822.33cd
Interface numbering subtype :
Interface number     : 0
Object identifier    :

LLDP-MED capabilities :
Device class        :
HardwareRev         :
FirmwareRev         :
SoftwareRev         :
SerialNum           :
Manufacturer name   :
Asset tracking identifier :

Port ID type        : Interface name
Port id             : GigabitEthernet 0/1
Port description    :

802.1 organizationally information
Port VLAN ID       : 1
Port and protocol VLAN ID (PPVID) : 1
  PPVID Supported   : YES
  PPVID Enabled     : NO
VLAN name of VLAN 1 : VLAN0001
Protocol Identity  :

802.3 organizationally information
Auto-negotiation supported : YES
Auto-negotiation enabled   : YES
PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full
duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode,
10BASE-T half duplex mode
Operational MAU type : speed(1000)/duplex(Full)
PoE support          : NO
Link aggregation supported : YES
Link aggregation enabled : NO
```



```

Aggregation port ID      : 0
Maximum frame Size      : 1500
LLDP-MED organizationally information
Power-via-MDI device type :
Power-via-MDI power source :
Power-via-MDI power priority :
Power-via-MDI power value :
    
```

Description of fields:

Field	Description
Neighbor index	Neighbor index
Device type	Type of neighboring device
Update time	Latest update time of neighbor information
Aging time	Aging time of a neighbor, namely the time after which a neighbor is aged and deleted
Chassis ID type	Chassis ID type
Chassis ID	Used to identify a device. Usually, a MAC address is used.
System name	Device name
System description	Device description, including hardware/software version and operating system
System capabilities supported	Functions supported by the system
System capabilities enabled	Functions enabled by the system
Management address subtype	Type of management address
Management address	Management address
Interface numbering subtype	Interface type of management address
Interface number	Interface ID of management address
Object identifier	Object ID of management address
Device class	MED device type: network connectivity device and terminal device Network connectivity device: Class I: general terminal device Class II: media terminal device, including capabilities of Class I and supporting media stream Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Manufacturer name
Asset tracking identifier	Asset ID
Port ID type	Port ID type
Port ID	Port ID

Port description	Port description
Port VLAN ID	VLAN ID of a port
Port and protocol VLAN ID	Port and protocol VLAN ID
PPVID Supported	Whether port and protocol VLAN is supported
PPVID Enabled	Whether port and protocol VLAN is enabled
VLAN name of VLAN 1	VLAN 1 name
Protocol Identity	Protocol ID
Auto-negotiation supported	Whether auto-negotiation is supported
Auto-negotiation enabled	Whether auto-negotiation is enabled
PMD auto-negotiation advertised	Port auto-negotiation advertisement capability
Operational MAU type	Rate and duplex status of port auto-negotiation
PoE support	Whether POE is supported
Link aggregation supported	Whether link aggregation is supported
Link aggregation enabled	Whether link aggregation is enabled
Aggregation port ID	ID of link aggregation port
Maximum frame Size	Maximum frame length supported by a port
Power-via-MDI device type	Device type, including: <ul style="list-style-type: none"> ● PSE ● PD
Power-via-MDI power source	Power type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Power value of a port where power is supplied

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

12.26 show lldp network-policy profile

Use this command to display the information about an LLDP network policy.

show lldp network-policy { **profile** [*profile-num*] | **interface** *interface-name* }

Parameter	Parameter	Description
Description	<i>profile-num</i>	ID of a network policy, in the range from 1 to 1024.
	<i>interface-name</i>	Interface name

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide If *profile-num* is specified, the information about the specified network policy is displayed.
If no parameter is specified, the information about all network policies is displayed.

Configuration Examples The following example displays the information about a network policy. Ruijie#

```
show lldp network-policy profile
network-policy information:
-----
Network Policy Profile 1
  voice vlan 2 cos 4 dscp 6
  voice-signaling vlan 2000 cos 4 dscp 6
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

12.27 show lldp statistics

The following example displays LLDP statistics.

show lldp statistics [**global** | **interface** *interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

- **global** parameter: display the global LLDP statistics.
- **Interface** parameter: display the LLDP statistics of the specified interface.

Configuration Examples The following example displays all LLDP statistics.

```
Ruijie# show lldp statistics
lldp statistics global Information:
Neighbor information last changed time : 1hour 52minute 22second
The number of neighbor information inserted : 2
The number of neighbor information deleted : 0
The number of neighbor information dropped : 0
The number of neighbor information age out : 1
```

```

-----
Lldp statistics information of port [GigabitEthernet 0/1]
-----
The number of lldp frames transmitted : 26
The number of frames discarded      : 0
The number of error frames          : 0
The number of lldp frames received  : 12
The number of TLVs discarded        : 0
The number of TLVs unrecognized     : 0
The number of neighbor information aged out : 0

```

show lldp statistics command output description:

Field	Description
Neighbor information last change time	Time the neighbor information is latest updated
The number of neighbor information inserted	Number of times of adding neighbor information
The number of neighbor information deleted	Number of times of removing neighbor information
The number of neighbor information dropped	Number of times of dropping neighbor information
The number of neighbor information aged out	Number of the neighbor information entries that have aged out
The number of lldp frames transmitted	Total number of the LLDPDUs transmitted
The number of frames discarded	Total number of the LLDPDUs discarded
The number of error frames	Total number of the LLDP error frames received
The number of lldp frames received	Total number of the LLDPDUs received
The number of TLVs discarded	Total number of the LLDP TLVs dropped
The number of TLVs unrecognized	Total number of the LLDP TLVs that cannot be recognized
The number of neighbor information aged out	Number of the neighbor information entries that have aged out

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

12.28 show lldp status

Use this command to display LLDP status information.

show lldp status [interface *interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	interface parameter: display the LLDP status information of the specified interface.	

Configuration Examples The following example displays LLDP status information of all ports.

```
Ruijie# show lldp status
Global status of LLDP      : Enable
Neighbor information last changed time : 1hour 52minute 22second
Transmit interval        : 30s
Hold multiplier          : 4
Reinit delay             : 2s
Transmit delay           : 2s
Notification interval    : 5s
Fast start counts        : 3
-----
Port [GigabitEthernet 0/1]
-----
Port status of LLDP      : Enable
Port state                : UP
Port encapsulation       : Ethernet II
Operational mode         : RxAndTx
Notification enable      : NO
Error detect enable      : YES
Number of neighbors      : 1
Number of MED neighbors   : 0
```

show lldp status command output description:

Field	Description
Global status of LLDP	Whether LLDP is globally enabled
Neighbor information last changed time	Time the neighbor information is latest updated
Transmit interval	LLDPDU transmit interval
Hold multiplier	TTL multiplier
Reinit delay	Port re-initialization delay
Transmit delay	LLDPDU transmit delay

Notification interval	Interval for sending LLDP Traps
Fast start counts	The number of fast sent LLDPDUs
Port status of LLDP	Whether LLDP is enabled on the port
Port state	Link status of port: UP or DOWN
Port encapsulation	LLDPDU encapsulation format
Operational mode	Operating mode of LLDP
Notification enable	Whether LLDP Trap is enabled on the port
Error detect enable	Whether error detection is enabled on the port
Number of neighbors	Number of neighbors
Number of MED neighbors	Number of MED neighbors

Related	Command	Description
Commands	N/A	N/A
Platform	N/A	
Description		

12.29 show lldp tlv-config

Use this command to display the advertisable TLV configuration of a port.

show lldp tlv-config [**interface** *interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide **Interface** parameter: display the LLDP TLV configuration of the specified interface.

Configuration Examples The following example displays TLV information of port 1.

```
Ruijie# show lldp tlv-config interface GigabitEthernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
-----
      NAME      STATUS  DEFAULT
-----
Basic optional TLV:
Port Description TLV      YES YES
System Name TLV          YES YES
System Description TLV    YES YES
```

```

System Capabilities TLV  YES YES
Management Address TLV  YES YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV       YES YES
Port And Protocol VLAN ID TLV  YES YES
VLAN Name TLV          YES YES

IEEE 802.3 extend TLV:
MAC-Physic TLV         YES YES
Power via MDI TLV      YES YES
Link Aggregation TLV   YES YES
Maximum Frame Size TLV YES YES

LLDP-MED extend TLV:
Capabilities TLV       YES YES
Network Policy TLV    YES YES
Location Identification TLV NO NO
Extended Power via MDI TLV YES YES
Inventory TLV         YES YES
    
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

13 QinQ Commands

13.1 dot1q new-outer-vlan *new-vid* translate old-outer-vlan *vid* inner-vlan *v-list*

Use this command to modify the policy list of outer vid based on the inner Tag VID and outer Tag VID on the access, trunk, hybrid, uplink port. Use the **no** form of this command to restore the default setting.

dot1q new-outer-vlan *new-vid* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*

no dot1q new-outer-vlan *new-vid* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*

Parameter Description	Parameter	Description
	new-vid	Vid list of the
	vid	Vid of outer tag.
	no	Removes the setting.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A.

Configuration Examples The following example modifies the vid to 3888 when the input packets inner tag vid.

```
Ruijie(config)# vlan 1888, 3888
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# dot1q new-outer-vlan 3888 translate old-outer-vlan 1888
inner-vlan 2001-3000
Ruijie(config-if)# end
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.2 dot1q outer-vid vid register inner-vid v-list

Use this command to configure the add policy list of outer vid based on protocol on tunnel port. Use the **no** or **default** form of this command to restore the default setting.

dot1q outer-vid *vid* **register inner-vid** *v_list*

no dot1q outer-vid *vid* **register inner-vid** *v_list*

Parameter Description	Parameter	Description
	<i>v_list</i>	Inner vlan id list
	<i>vid</i>	Outer vlan id list
	no	Removes the settings.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies vid in the tag of input message as 4-22 and sets the vid to 3.

```
Ruijie#configure
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport mode dot1q-tunnel
Ruijie(config-if)#dot1q outer-vid 3 register inner-vid 4-22
Ruijie(config-if)#end
```

Related Commands	Command	Description
	show registration-table [interface <i>intf-id</i>]	N/A

Platform N/A

Description

13.3 dot1q relay-vid vid translate local-vid v-list

Use this command to configure the modify policy list of outer vid based on protocol on access, trunk, hybrid port. Use the **no** or **default** form of this command to restore the default setting.

dot1q relay-vid *vid* **translate local-vid** *v-list*

no dot1q relay-vid *vid* **translate local-vid** *v-list*

default dot1q relay-vid *vid* **translate local-vid** *v-list*

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
v_list	Outer vlan list of input message
vid	Modified outer vlan id list
no	Removes the settings.

Defaults The policy list is null by default.

Command Interface configuration mode.

Mode

Usage Guide N/A

Configuration Examples The following example specifies vid in the outer tag of input message as 10-20 and sets the vid to 100.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# dot1q relay-vid 100 translate local-vid 10-20
Ruijie(config-if)# end
```

Related Commands	Command	Description
	show translation-table [interface <i>intf-id</i>]	N/A

Platform N/A

Description

13.4 dot1q relay-vid vid translate inner-vid v-list

Use this command to configure the modify policy list of outer vid based on protocol on access, trunk, hybrid port. Use the **no** or **default** form of this command to restore the default setting.

dot1q relay-vid *vid* **translate** **inner-vid** *v-list*

no dot1q relay-vid *vid* **translate** **inner-vid** *v-list*

default dot1q relay-vid *vid* **translate** **inner-vid** *v-list*

Parameter Description	Parameter	Description
	v_list	Outer vlan list of input message
	vid	Modified outer vlan id list
	no	Removes the settings.

Defaults The policy list is null by default.

Command Interface configuration mode.

Mode**Usage Guide** N/A**Configuration Examples** The following example configures vid in the outer tag of input message as 10-20 and sets the vid to 100.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# dot1q relay-vid 100 translate inner-vid 10-20
Ruijie(config-if)# end
```

Related Commands

Command	Description
show translation-table [interface <i>intf-id</i>]	N/A

Platform N/A**Description**

13.5 dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

Use this command to map the priority from the outer tag to the inner tag for the packets on the interface. Use the **no** form of this command to restore the default setting.

dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value**no dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value****default dot1q-Tunnel cos *inner-cos-value* remark-cos *outer-cos-value***

Parameter	Parameter	Description
Description	<i>inner-cos-value</i>	Indicates the CoS value of the inner tag.
	<i>outer-cos-value</i>	Indicates the CoS value of the outer tag.
	no	Cancels the priority mapping of the packets on the interface.

Defaults The policy list is null by default.**Command** Interface configuration mode.**Mode****Usage Guide** If the QoS policy based on the COS value is set for the service provider's network to which a user network connects, the COS value of the outer tag can be set to different values based on the data packet importance. In this case, important services can be preferentially processed and transmitted.**Configuration Examples** The following example configures the priority mapping from the outer tag to the inner tag.

```
ruijie# configure
ruijie(config)# interface gigabitEthernet 0/2
ruijie(config-if)# dot1q-tunnel cos 3 remark-cos 5
```

```
ruijie(config-if)# end
```

**Related
Commands**

Command	Description
show interface intf-name remark	N/A

Platform N/A

Description

13.6 frame-tag tpid

Use this command to set the packet TPID compatible with the manufacturer TPID. Use the **no** or **default** form of this command to restore the default setting.

frame-tag tpid tpid

no frame-tag tpid

default frame-tag tpid

**Parameter
Description**

Parameter	Description
tpid	Packet TPID.
no	Removes the setting.

Defaults The default is 0x8100.

**Command
Mode** Interface configuration mode.

Usage Guide If the TPID value of the connected third-party device is not 0x8100 (default value) defined in IEEE802.1Q, the TPID value on the egress used to connect to the third-party device is the TPID value of the third-party device.

Configuration The following example sets the packet TPID compatible with the manufacturer TPID.

Examples

```
Ruijie(config)# interface g0/3
Ruijie(config-if)# frame-tag tpid 0x9100
Ruijie(config-if)# end
Ruijie# show frame-tag tpid
Port      tpid
-----  -
Gi0/3     0x9100
```

**Related
Commands**

Command	Description
show frame-tag tpid	N/A

Platform N/A
Description

13.7 inner-priority-trust enable

Use this command to copy the priority of the inner tag to the outer tag of the packets on the interface. Use the **no** or **default** form of this command to restore the default setting.

inner-priority-trust enable
no inner-priority-trust enable
default inner-priority-trust enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Interface configuration mode.
Mode

Usage Guide If the QoS policy is configured based on the COS value of the user's VLAN tag for the service provider's network to which a user network connects, the user's VLAN tag priority can be copied to the outer VLAN tag, so that the user's packets are encapsulated with the outer VLAN tag and have the same priority as the user's VLAN tag. In this case, the user's packets can be preferentially processed and transmitted on the service provider's network.

Configuration Examples The following example copies the priority of the inner tag to the outer tag of the packets on the interface.

```
ruijie#configure terminal
ruijie(config)# interface gigabitEthernet 0/2
ruijie(config-if)# inner-priority-trust enable
ruijie(config-if)#end
```

Related Commands	Command	Description
	show inner-priority-trust	N/A

Platform N/A
Description

13.8 l2protocol-tunnel

Use this command to set the dot1q-tunnel port to receive L2 protocol message. Use the **no** or **default**

form of this command to disable this function.

```
l2protocol-tunnel { stp | gvrp }
no l2protocol-tunnel { stp | gvrp }
default l2protocol-tunnel { stp | gvrp }
```

Parameter Description	Parameter	Description
	stp	Receives stp message.
	gvrp	Receives gvrp message.
	no	Removes the settings.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide If the STP and GVRP packets need to be transparently transmitted, this function must be enabled in global configuration mode.

Configuration Examples The following example enables the function of receiving L2 protocol gvrp and stp.

```
Ruijie#configure
Ruijie(config)# l2protocol-tunnel stp
Ruijie(config)# l2protocol-tunnel gvrp
Ruijie(config)#end
```

Related Commands	Command	Description
	show l2protocol-tunnel { gvrp stp }	N/A

Platform N/A

Description

13.9 l2protocol-tunnel enable

Use this command to enable transparent transmission of L2 protocol message. Use the **no** or **default** form of this command to restore the default setting.

```
l2protocol-tunnel { stp | gvrp } enable
no l2protocol-tunnel { stp | gvrp } enable
```

Parameter Description	Parameter	Description
	stp	Transparently transmits stp message.
	gvrp	Transparently transmits gvrp message.

no	Removes the settings.
-----------	-----------------------

Defaults It is disabled by default.

Command Mode Interface configuration mode.

Usage Guide 1 If this function is enabled in global and interface configuration modes, STP packets can be transparently transmitted after the bridge-frame forwarding protocol bpdud command is enabled in global configuration mode.

Configuration Here is an example of enabling transparent transmission of L2 protocol message :

Examples

```
Ruijie#configure
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# l2protocol-tunnel gvrp enable
Ruijie(config-if)#end
```

Related Commands

Command	Description
show l2protocol-tunnel { gvrp stp }	N/A

Platform N/A
Description

13.10 l2protocol-tunnel tunnel-dmac

Use this command to set the MAC address for the transparent transmission of the corresponding protocol messages. Use the **no** or **default** form of this command to restore the default setting.

l2protocol-tunnel { stp|gvrp } tunnel-dmac mac-address

no l2protocol-tunnel { stp|gvrp } tunnel-dmac mac-address

default l2protocol-tunnel { stp | gvrp } tunnel-dmac mac-address

Parameter Description

Parameter	Description
stp	Sets the STP transparent transmission address.
gvrp	Sets the GVRP transparent transmission address.
<i>mac-address</i>	Sets the transparent transmission address.
no	Restore the transparent transmission address to the default value. If OUI is 001aa9 or 00d0f8, the first three bytes of the default transparent transmission address is 01d0f8, the last three bytes is 000005 for STP and 000006 for GVRP. If OUI is not 001aa9 and 00d0f8, the first three bytes is 01d0f8, the last three bytes is 000005 for STP and 000006 for GVRP.

Defaults The first three bytes of the address are 01d0f8 and the last three bytes are 000005 for **stp** and 000006 for **gvrp** by default.

Command Global configuration mode.

Mode

Usage Guide N/A

Configuration The following example sets the MAC address for the L2-protocol transparent transmission function:

Examples

```
ruijie# configure terminal
Ruijie(config-if)# l2protocol-tunnel gvrp tunnel-dmac 011AA9 000005
Ruijie(config-if)#end
```

**Related
Commands**

Command	Description
show l2protocol-tunnel { gvrp stp }	N/A

Platform N/A

Description

13.11 mac-address-mapping x source-vlan *src-vlan-list* destination-vlan *dst-vlan-id*

Use this command to copy the MAC address dynamically-learned from the source VLAN to the destination VLAN. Use the **no** or **default** form of this command to restore the default setting.

mac-address-mapping x source-vlan *src-vlan-list* destination-vlan *dst-vlan-id*

no mac-address-mapping x source-vlan *src-vlan-list* destination-vlan *dst-vlan-id*

default mac-address-mapping x source-vlan *src-vlan-list* destination-vlan *dst-vlan-id*

**Parameter
Description**

Parameter	Description
index-id	Policy ID of copying MAC addresses.
src-vlan-list	Source VLAN list of copying MAC addresses.
dst-vlan-id	Destination VLAN ID of copying MAC addresses.

Defaults This function is disabled by default.

Command Interface configuration mode.

Mode

Usage Guide N/A

Configuration The following example copies the MAC addresses dynamically-learned from the source VLANs 1-3 to the destination VLAN 5.

Examples

```
ruijie#configure
ruijie(config)# interface gigabitEthernet 0/2
ruijie(config-if) # mac-address-mapping 1 source-vlan 1-3 destination-vlan 5
ruijie(config-if) #end
```

Related Commands

Command	Description
show interface mac-address-mapping x	N/A

Platform N/A

Description

13.12 show dot1q-tunnel

Use this command to display whether dot1q-tunnel of interface is enabled or not.

show dot1q-tunnel [interface *intf-id*]

Parameter Description

Parameter	Description
intf-id	The specified interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays whether dot1q-tunnel of interface is enabled or not.

Examples

```
Ruijie# show dot1q-tunnel
Ports   Dot1q-tunnel
-----  -
Gi0/1   Enable
```

Related Commands

Command	Description
N/A	N/A

Platform

Description

13.13 show frame-tag tpid

Use this command to display the configuration of interface tpid.

show frame-tag tpid [**interface** <intf-id>]

Parameter Description	Parameter	Description
	intf-id	Specifies the interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays the configuration of interface tpid.

Examples

```
Ruijie# show frame-tag tpid
Ports      tpid
-----  -----
Gi0/1      0x9100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.14 show inner-priority-trust

Use this command to display whether the priority copy function is enabled.

show inner-priority-trust

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays whether the priority copy function is enabled.

Examples

```
Ruijie# show inner-priority-trust
Port      inner-priority-trust
-----  -----
Gi0/1     enable
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

13.15 show interface dot1q-tunnel

Use this command to display the VLAN configuration on the dot1q-tunnel port.

show interface [*intf-id*] dot1q-tunnel

**Parameter
Description**

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A

**Command
Mode** Any mode

Usage Guide N/A

Configuration The following example displays the VLAN configuration on the dot1q-tunnel port.

Examples

```
Ruijie# show interfaces dot1q-tunnel
Interface: Gi0/3
Native vlan: 10
Allowed vlan list: 4-6, 10, 30-60
Tagged vlan list: 4, 6, 30-60
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

13.16 show interface mac-address-mapping

Use this command to display the MAC address mapping configuration.

show interface mac-address-mapping

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays the MAC address mapping configuration.

Examples

```
ruijie# show interface mac-address-mapping
Ports      Status    Index    Destination-VID Source-VID-list
-----
Gi0/1      active    2        3          2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.17 show interface remark

Use this command to display the priority mapping configuration.

show interface [*intf-id*] remark

Parameter Description	Parameter	Description
	<i>intf-id</i>	specifies an interface

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays the priority mapping configuration.

Examples

```
Ruijie# show interface remark
Ports          Type          From value  To value
-----
Gi0/1          Cos-To-Cos   3           5
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

13.18 show interfaces dot1q-tunnel

Use this command to display the VLAN configuration on the dot1q-tunnel port.

show interfaces [intf-Id] dot1q-tunnel

Parameter Description

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays the VLAN configuration on the dot1q-tunnel port.

Examples

```
Ruijie# show interfaces dot1q-tunnel
Interface: Gi0/3
Native vlan: 10
Allowed vlan list: 4-6, 10, 30-60
Tagged vlan list: 4, 6, 30-60
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

13.19 show interfaces mac-address-mapping

Use this command to display the MAC address mapping configuration.

show interfaces mac-address-mapping

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays the MAC address mapping configuration.

Examples

```
ruijie# show interfaces mac-address-mapping
Ports      Status    Index    Destination-VID Source-VID-list
-----
Gi0/1      active    2        3          2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.20 show interfaces remark

Use this command to display the priority mapping configuration.

show interfaces [*intf-id*] remark

Parameter Description	Parameter	Description
	<i>intf-id</i>	specifies an interface

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays the priority mapping configuration.

Examples

```
Ruijie# show interface remark
Ports          Type          From value  To value
-----
Gi0/1         Cos-To-Cos   3           5
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

13.21 show l2protocol-tunnel

Use this command to display transparent transmission configuration of L2 protocol.

show l2protocol-tunnel { gvrp | stp }

**Parameter
Description**

Parameter	Description
gvrp	Displays configuration of transparently transmitting gvrp protocol.
stp	Displays configuration of transparently transmitting stp protocol.

Defaults N/A

**Command
Mode** Any mode

Usage Guide N/A

Configuration The following example displays transparent transmission configuration of L2 protocol.

Examples

```
Ruijie# show l2protocol-tunnel stp
L2protocol-tunnel: Stp Enable
Ruijie# show l2protocol-tunnel gvrp
L2protocol-tunnel: gvrp Disable
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

13.22 show registration-table

Use this command to display vid add policy list of prorocol-based dot1q-tunnel port.

show registration-table [interface *intf-id*]

Parameter Description	Parameter	Description
	intf-id	Specifies the interface.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration The following example displays vid add policy list of prorocol-based dot1q-tunnel port.

Examples

```
Ruijie# show registration-table
Ports      Type      Outer-VID Inner-VID-list
-----
Gi0/7      Add-outer 5          7-10,15,20-30
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.23 show traffic-redirect

Use this command to display flow-based vid change or add policy list.

show traffic-redirect [interface *intf-id*]

Parameter Description	Parameter	Description
	intf-id	Specifies the interface.

Defaults N/A

Command Any mode

Mode**Usage Guide** N/A**Configuration** The following example displays flow-based vid change or add policy list.**Examples**

```
Ruijie# show traffic-redirect
Ports          Type          VID  Match-filter
-----
Gi0/3          Mod-outer     23   11
Gi0/3          Mod-outer     3    4
Gi0/3          Mod-outer     6    5
Gi0/3          Mod-inner     8    inner-to-8
Gi0/6          Mod-inner     9    100
Gi0/7          Nested-vid    13   nest-13
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A**Description**

13.24 show translation-table

Use this command to display vid modify policy list of protocol-based access, trunk, hybrid port.

show translation-table [interface *intf-id*]**Parameter
Description**

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A**Command** Any mode**Mode****Usage Guide** N/A**Configuration** The following example displays vid modify policy list of protocol-based access, trunk, hybrid port.**Examples**

```
Ruijie# show translation-table
Ports          Type          Relay-VID  Old-local  Local\inner-VID-list
-----
Gi0/7          Inner-CVID    8          N/A        10-20
Gi0/7          Local-SVID    1001       N/A        30-60
```

Gi0/7	In+Out	8	20	50
-------	--------	---	----	----

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

13.25 switchport dot1q-tunnel allowed vlan

Use this command to configure the allowed VLAN of dot1q-tunnel. Use the **no** or **default** form of this command to restore the default setting.

switchport dot1q-tunnel allowed vlan { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* }

no switchport dot1q-tunnel allowed vlan

default switchport dot1q-tunnel allowed vlan

Parameter Description

Parameter	Description
add	Add allowed VLAN.
tagged	Tag-carried.
untagged	Not tag-carried.
<i>v_list</i>	vlan id list.
no	Remove the settings.

Defaults The default is **untagged 1**.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies vlan 3-6 of dot1q-tunnel port as allowed VLAN and outputting the frame with tag.

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport dot1q-tunnel allowed vlan tagged 3-6
Ruijie(config)#end
```

Related Commands

Command	Description
show interface dot1q-tunnel	N/A

Platform N/A

Description

13.26 switchport dot1q-tunnel native vlan

Use this command to configure the default vlan id of dot1q-tunnel. Use the **no** or **default** form of this command to restore the default setting.

switchport dot1q-tunnel native vlan *vid*

no switchport dot1q-tunnel native vlan

default switchport dot1q-tunnel native vlan

Parameter	Parameter	Description
Description	vid	Configures default vlan id.
	no	Configures default vlan as 1.

Defaults The default is VLAN 1.

Command Interface configuration mode.

Mode

Usage Guide N/A

Configuration The following example specifies default VLAN of dot1q-tunnel port as 8.

Examples

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport dot1q-tunnel native vlan 8
Ruijie(config)#end
```

Related Commands	Command	Description
	show interface dot1q-tunnel	N/A

Platform N/A

Description

13.27 switchport mode dot1q-tunnel

Use this command to configure the interface as the dot1q-tunnel interface. Use the **no** or **default** form of this command to restore the default setting.

switchport mode dot1q-tunnel

no switchport mode

default switchport mode

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
	no Deletes the corresponding dot1q-tunnel interface configuration.

Defaults The interface is not a tunnel port by default.

Command Interface configuration mode.

Mode

Usage Guide N/A

Configuration The following example configures the interface as the dot1q-tunnel interface.

Examples

```
ruijie(config)# interface gigabitEthernet 0/1
ruijie(config-if)# switchport mode dot1q-tunnel
ruijie(config)# end
```

Related Commands	Command	Description
	show vlan	N/A

Platform N/A

Description

13.28 traffic-redirect access-group *acl* inner-vlan *vid* out

Use this command to configure the modification policy of inner vid based on flow for the packets outputted from the access, trunk, hybrid port. Use the **no** or **default** form of this command to restore the default setting.

traffic-redirect access-group *acl* inner-vlan *vid* out

no traffic-redirect access-group *acl* inner-vlan

default traffic-redirect access-group *acl* inner-vlan

Parameter Description	Parameter	Description
	<i>acl</i>	Flow matching.
	<i>vid</i>	Modified inner vid
	no	Removes the settings.

Defaults By default, no policy is configured.

Command Interface configuration mode.

Mode

Usage Guide N/A

Configuration The following example specifies the outer vid of outgoing messages whose source address is 1.1.1.2 as 6,

Examples

```
Ruijie#configure
Ruijie(config)#ip access-list standard to_6
Ruijie(config-std-nacl)#permit host 1.1.1.2
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# traffic-redirect access-group to_6 inner-vlan 6 out
Ruijie(config-if)# end
```

Related Commands

Command	Description
show traffic-redirect	N/A

Platform N/A

Description

13.29 traffic-redirect access-group acl nested-vlan vid in

Use this command to configure vid add policy list based on flow on dot1q-tunne port. Use the **no** or **default** form of this command to restore the default setting.

traffic-redirect access-group acl nested-vlan vid in

no traffic-redirect access-group acl nested -vlan

default traffic-redirect access-group acl nested -vlan

Parameter Description

Parameter	Description
<i>acl</i>	Flow matching.
<i>vid</i>	vid list to be added.
no	Removes the settings.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Mode

Usage Guide N/A

Configuration The following example specifies the vid of input message whose source address is 1.1.1.3 as 9.

Examples

```
Ruijie#configure
Ruijie(config)#ip access-list standard 20
Ruijie(config-std-nacl)#permit host 1.1.1.3
Ruijie(config-std-nacl)#exit
```

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# traffic-redirect access-group 20 nested-vlan 10 in
Ruijie(config-if)# end
```

**Related
Commands**

Command	Description
show traffic-redirect	N/A

Platform N/A
Description

13.30 traffic-redirect access-group acl outer-vlan vid in

Use this command to configure the modify policy list of outer vid based on flow on access, trunk, hybrid port. Use the **no** or **default** form of this command to restore the default setting.

traffic-redirect access-group acl outer-vlan vid in

no traffic-redirect access-group acl outer-vlan

default traffic-redirect access-group acl outer-vlan

**Parameter
Description**

Parameter	Description
<i>acl</i>	Flow matching.
<i>vid</i>	Modified outer vid list
no	Removes the settings.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies outer vid of input message whose source address is 1.1.1.1 as 3.

```
Ruijie# configure
Ruijie(config)# ip access-list standard 2
Ruijie(config-std-nacl)# permit host 1.1.1.1
Ruijie(config-std-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
Ruijie(config-if)# end
```

**Related
Commands**

Command	Description
show traffic-redirect	N/A

**Platform
Description**

N/A

14 ERPS Commands

14.1 associate sub-ring

Use this command to associate the ethernet ring with its sub-rings.

associate sub-ring raps-vlan *vlan-list*

no associate sub-ring raps-vlan *vlan-list*

Parameter Description	Parameter	Description
	<i>vlan-list</i>	Sub-rings' R-APS VLAN.

Defaults By default, Ethernet ring is not associated with its sub-rings.

Command ERPS configuration mode.

Mode

Usage Guide

1. You need to configure this command on all nodes of the Ethernet ring, so as to transmit its sub-ring's ERPS protocol packets in the Ethernet ring.
2. Configuring the association is mainly to make the sub-ring's protocol packets transmit in the Ethernet ring. Users can also adopt the configuration command provided by the VLAN module to configure elaborately the VLAN and the relation between ports and VLAN, so as to transmit the sub-ring's protocol packets in other Ethernet rings and not leak the packets to the user network.

Configuration The following example associates the Ethernet sub-ring with other Ethernet rings:

Examples

```
#Enter the privileged EXEC mode
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

# Configure the link mode of the Ethernet ring port and the default VLAN.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit

# Enter the erps configuration mode.
Ruijie(config)# erps raps-vlan 4093

#Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet
```



```

0/2

# Configure the Ethernet subring
Ruijie(config)# erps raps-vlan 100
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel
Ruijie(config-if)# exit

# Associate the subring with other Ethernet rings.
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)# associate sub-ring raps-vlan 100

```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

14.2 erps enable

Use this command to enable/disable the ERPS function in the global configuration mode.

erps enable

no erps enable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults Disabled

**Command
Mode** Global configuration mode.

Usage Guide The ERPS protocol of the specified ring will begin running truly only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled.

Configuration The following example enables the ERPS protocol globally:

Examples

```

# Enter the privileged EXEC mode
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```

```
# Enable the ERPS function globally.
Ruijie(config)# erps enable
```

```
# Enter the ERPS configuration mode
Ruijie(config)# erps raps-vlan 4093
```

```
# Enable the ERPS function for the specified ring.
Ruijie(config-erps4093)# state enable
```

Related Commands

Command	Description
state enable	After entering the ERPS configuration mode of the specified ring, configure this command to enable the ERPS protocol of this specified ring.

Platform N/A

Description

14.3 erps monitor link-state by oam

Use this command to configure the method of monitoring the ERPS link state.

erps monitor link-state by oam *vlan* *vlan-id*

no erps monitor link-state by oam

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, it adopts the directly monitoring the link physical state (up or down) rather than the oam method.

Command Mode Global configuration mode.

Usage Guide For the link state monitoring, use the method of directly monitoring the link physical state (up or down), also monitor the logic state (unidirectional fault, bidirectional fault or normal) of the link by the OAM. By default, the former is adopted. If the OAM method is used, the inefficient link state monitoring may cause the convergence time longer when the topology changes.

Configuration Examples The following example configures the method of monitoring the link state.

```
# Enter the privileged EXEC mode.
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
# Configure the method of monitoring the link state.
Ruijie(config)# erps monitor link-state by oam vlan 100
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

14.4 erps raps-vlan

Use this command to configure the R-APS VLAN of Ethernet ring.

erps raps-vlan *vlan-id*

no erps raps-vlan *vlan-id*

**Parameter
Description**

Parameter	Description
<i>vlan-id</i>	R-APS VLAN ID

Defaults

No R-APS VLAN is configured.

**Command
Mode**

Global configuration mode.

Usage Guide

The R-APS VLAN must be the VLAN that is not used on the device. Cannot set the VLAN1 to the R-APS VLAN.

The same Ethernet ring of different devices needs the same R-APS VLAN.

If you want to transparently transmit the ERPS protocol packets on a device without the ERPS function configured, make sure that only the two ports connected to the Ethernet ring on this device allow the R-APSA VLAN packets corresponding to this ERPS ring passing through. Otherwise, the other VLAN packets may enter the R-APS VLAN through the transparent transmission, causing the shock to the ERPS ring.

Configuration

```
# Enter the privileged EXEC mode.
```

Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

#Configure the R-APS VLAN globally.
Ruijie(config)# erps raps-vlan 4093
```

**Related
Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

Platform N/A

Description

14.5 protected-instance

Use this command to configure the VLAN protected by the Ethernet ring to implement the load balance function.

protected-instance *instance-id-list*

no protected-instance

Parameter Description	Parameter	Description
	<i>instance-id-list</i>	Instance protected by this Ethernet ring. (The VLANs corresponding to these instances are the VLANs protected by the Ethernet ring.)

Defaults By default, all VLANs are protected.

Command ERPS configuration mode.

Mode

Usage Guide The protected VLAN consists of the R-APS VLAN of this Ethernet ring and the data VLAN protected by this Ethernet ring.

Configuration Examples Suppose that the ERP1 and ERP2 are configured on the switch to implement the load balance. The R-APS VLAN of the ERPS1 is 100, the protected data VLAN is in the range of 1 to 99 and 101-2000, the R-APS VLAN of the ERPS2 is 4093, and the protected data VLAN is in the range of 2001 to 4092 and 4094. Configuration for the load balance is shown as below:

```
# Enter the privileged EXEC mode.
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
# Configure the VLAN configured by the ERP1.
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 100, 1-99, 101-2000
Ruijie(config-mst)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)#protected-instance 1
```

```
# Configure the VLAN configured by the ERP2.
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 2 vlan 4093, 2001-4092, 4094
Ruijie(config-mst)# exit
```

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)#protected-instance 2
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

14.6 ring-port

Use this command to configure the ERPS ring.

```
ring-port west { interface-name1 | virtual-channel } east { interface-name2 | virtual-channel }
no ring-port
```

Parameter Description

Parameter	Description
<i>interface-name1</i>	Name of the West port.
<i>interface-name2</i>	Name of the East port.

Defaults No ERPS ring is configured.

Command Mode EPRS configuration mode.

Usage Guide

- 1) After adding the port to the ERP ring, the trunk attribute of the port is not allowed to be modified any more.
- 2) If the ring port is configured on the virtual-channel, this ring will be considered as a sub-ring.
- 3) Ports running the ERPS do not participate in the STP computing. ERPS, RERP and REUP do not share the port.

Configuration The following example is for the ERPS ring.

Examples

```
# Enter the privileged EXEC mode.
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
# Configure the link mode of the Ethernet ring port and the default VLAN.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

```
# Enter the ERPS configuration mode.
Ruijie(config)# erps raps-vlan 4093
```

```
#Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet
0/2
```

Related Commands

Command	Description
state enable	Enable the ERPS protocol of the specified ring in the ERPS mode of the specified ring.
sub-ring associate raps-vlan <i>vlan-id</i>	Establish the association between the subring and other Ethernet rings in the subring ERPS configuration mode.

Platform N/A

Description

14.7 rpl-port

Use this command to configure the RPL port and RPL owner.

```
rpl-port { west | east } [ rpl-owner ]
no rpl-port
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults No RPL port and RPL owner are configured.

Command Mode EPRS configuration mode.

Usage Guide Up to one RPL link and one RPL owner node are needed and configurable for each ring.

Configuration Examples The following example configures the RPL port and RPL owner.

```
# Enter the privileged EXEC mode.
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
# Configure the link mode of the Ethernet ring port and the default VLAN.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
```

```
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

```
# Enter the ERPS configuration mode.
Ruijie(config)# erps raps-vlan 4093
```

```
# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

```
# Specify the port where the RPL link is and the RPL owner.
Ruijie(config-erps4093)# rpl-port west rpl-owner
```

Related Commands

Command	Description
ring-port west { <i>interface-name1</i> virtual-channel } east { <i>interface-name2</i> virtual-channel }	Configure the specified ERP ring in the ERPS configuration mode of the specified ring.
state enable	Enable the ERPS protocol of the specified ring in the ERPS configuration mode of the specified ring.

Platform N/A

Description

14.8 show erps

Use this command to show the parameters and states of the ERPS.

```
show erps [ { global | raps_vlan vlan-id [ sub-ring ] } ]
```

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example shows the use of this command.

Examples

```

Ruijie# show erps
ERPS Information
Global Status           : Enabled
Link monitored by      : Not Oam
-----
R-APS VLAN             : 4092
Ring Status            : Enabled
West Port              : Gi 0/5 (Blocking)
East Port              : Gi 0/7 (Forwarding)
RPL Port               : West Port
RPL Port Blocked VLAN : All
RPL Owner              : Enabled
Holdoff Time           : 0 milliseconds
Guard Time            : 500 milliseconds
WTR Time               : 5 minutes
Current Ring State     : Idle
-----
R-APS VLAN             : 4093
Ring Status            : Enabled
West Port              : Virtual Channel
East Port              : Gi 0/10 (Forwarding)
RPL Port               : None
RPL Port Blocked VLAN : All
RPL Owner              : Disabled
Holdoff Time           : 0 milliseconds
Guard Time            : 500 milliseconds
WTR Time               : 5 minutes
Current Ring State     : Idle
-----
R-APS VLAN             : 4094
Ring Status            : Enabled
West Port              : Virtual Channel
East Port              : 12 (Forwarding)
RPL Port               : None
RPL Port Blocked VLAN : All
RPL Owner              : Disabled
Holdoff Time           : 0 milliseconds
Guard Time            : 500 milliseconds
WTR Time               : 5 minutes
Current Ring State     : Idle

Ruijie# show erps raps_vlan 4093 sub-ring
R-APS VLAN: 4093
Sub-Ring R-APS VLANs   TC Propagation State

```


100	Enable
200	Enable

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

14.9 state enable

Use this command to enable/disable the specified R-APS ring.

state enable

no state enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled

Command Mode

EPRS configuration mode.

Usage Guide

Only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled, the ERPS protocol of the specified ring will begin truly running.

Configuration Examples

The following example enables the specified ERPS ring:

```
#Enter the privileged EXEC mode.
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

#Configure the link mode of the Ethernet ring port and the default VLAN.
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit

# Enter the ERPS configuration mode.
Ruijie(config)# erps raps-vlan 4093
```

```
# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet
0/2

# Enable the ERPS function for the specified ring.
Ruijie(config-erps4093)#state enable

# Enable the global ERPS function.
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

Related Commands

Command	Description
erps enable	Enable the global ERPS protocol.

Platform N/A
Description

14.10 sub-ring tc-propagation

Use this command to specify the devices corresponding to the crossing node on the crossing ring whether to send out the notification when the subring topology changes.

- sub-ring tc_propagation enable**
- no sub-ring tc_propagation**

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the topology changing notification is not sent.

Command Mode EPRS configuration mode.

Usage Guide This command is just needed to be configured on the crossing nodes on the crossing ring.

Configuration Examples The following example is configured when the subring topology changes.

```
# Enter the privileged EXEC mode.
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

#Configure the link mode of the Ethernet ring port and the default VLAN.
Ruijie(config)# interface fastEthernet 0/1
```

```

Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit

# Enter the ERPS configuration mode.
Ruijie(config)# erps raps-vlan 4093

# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.
Ruijie(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet
0/2

#Configure the Ethernet subring.
Ruijie(config)# erps raps-vlan 100
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel

# Associate the subring with other Ethernet rings.
Ruijie(config-erps100)# sub-ring associate raps-vlan 4093

# Enable the topology changing notification for the subring.
Ruijie(config-erps100)# sub-ring tc-propagation enable

```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.11 timer

Use this command to configure the timer of the ERPS protocol.

timer { **holdoff-time** *interval1* | **guard-time** *interval2* | **wtr-time** *interval3* }

no timer { **holdoff-time** | **guard-time** | **wtr-time** }

Parameter Description

Parameter	Description
interval1	Value of the Holdoff timer in 100 milliseconds, the valid range is 0 to 100.

Interval2	Value of the Guard timer in 10 milliseconds, the valid range is 1 to 200.
Interval3	Value of the WTR in minute, the valid range is 5 to 12.

Defaults Holdoff timer: 0.
 Guard timer: 500 milliseconds.
 WTP timer: 5 seconds.

Command EPRS configuration mode.
Mode

Usage Guide **Holdoff timer:** This timer is used to avoid the ERPS from topology switching continuously due to the link intermittent fault. With this timer configured, if the link fault is detected, the ERPS does not perform the topology switching immediately until the timer times out and the link fault is verified.
Guard timer: This timer is used to prevent the device receiving the timed-out R-APS messages. When the device detects the recovery from failure of the link, it sends out the message of link recovery and starts up the Guard timer. Before the Guard times out, except for the flush packets indicating the subring topology change, other packets are discarded directly without being handled.
WTR (Wait-to-restore) timer: This timer is only valid for the RPL owner device. It is mainly used to prevent the RPL owner making the erroneous judgment to the ring network status. When the RPL detects the fault recovery, it does not perform the topology switching immediately until the WTR times out and the Ethernet ring indeed recovers from the fault. If the ring network fault is checked again before the WTR times out, then the WTR timer will be canceled and topology switching will be not executed any longer.

Configuration The following example configures the timer of the ERPS protocol.

```
Examples # Enter the privileged EXEC mode.
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
# Enter the ERPS configuration mode.
Ruijie(config)# erps raps-vlan 4093

# Configure the protocol timer.
Ruijie(config-erps4093)# timer holdoff-time 10
Ruijie(config-erps4093)# timer guard-time 10
Ruijie(config-erps4093)# timer wtr-time 10
```

Related Commands	Command	Description
		N/A

Platform N/A
Description



IP Address & Application Commands

1. IP Address/Service Commands
2. ARP Commands
3. IPv6 Commands
4. DHCP Commands
5. DHCPv6 Commands
6. DNS Commands
7. FTP Server Commands
8. FTP Client Commands
9. Tunnel Commands
10. Network Connectivity Test Tool Commands
11. TCP Commands
12. IPv4/IPv6 REF Commands

1 IP Address/Service Commands

1.1 gateway

Use this command to set the gateway address for the management port. Use the **no** form of this command to remove the setting.

gateway *address*

no gateway

Parameter	Parameter	Description
Description	<i>address</i>	Sets the gateway address for the management port

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the gateway address for the management port to 1.1.1.1.

```
Ruijie(config)# interface mgmt 0
Ruijie(config-if-Mgmt 0)# gateway 1.1.1.1
Ruijie(config-if-Mgmt 0)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.2 ip-address

Use this command to configure the IP address of an interface. Use the **no** form of this command to restore the default setting.

ip address *ip-address network-mask* [**secondary**] | [**slave**]

no ip address *ip-address network-mask* [**secondary**] | [**slave**]

Parameter Description	Parameter	Description
	<i>ip-address</i>	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.

<i>network-mask</i>	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.
slave	Slave IP address.
secondary	Secondary IP address

Defaults No IP address is configured for the interface by default.

Command Interface configuration mode

Mode

Usage Guide The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value “1” are the network address. The IP address bits that correspond to value “0” are the host address. For example, the network mask of Class A IP address is “255.0.0.0”. You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The RGOS software supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary/slave IP addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses. The secondary IP address and the primary IP address must belong to the same network or different networks. Secondary IP addresses are often used in network construction. Typically, you can try to use secondary IP addresses in the following situations:

A network hasn’t enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured.

Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet.

Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces of a device.

Slave IP address is applied to the gateway cluster scenario. Only after the primary IP address is

configured can the slave IP address be configured. Both slave and primary addresses are configured on an Layer 3 interface, backing up each other. In general, the master device adopts the primary IP address and the slave device uses the slave IP address. When the slave device becomes the master, its IP address becomes the primary IP address. When the master device turns into a slave, its IP address becomes the slave IP address,

In general, the layer-2 switch is configured a default gateway with the **ip default-gateway** command. Sometimes the layer-2 switch may be managed through the telnet, and the management IP and default gateway of the layer-2 switch needed to be modified. In this case, after configuring any one of the **ip address** and **ip default-gateway** command, the other cannot be configured any more due to the configuration change which causes failing to access this device through the network. So you need to use the keyword **gateway** in the **ip address** command to modify both the management IP and default gateway. The keyword **gateway** is not in the output of **show running config**, but in the output of **ip default-gate** command.

Configuration Examples

The following example configures the primary IP address and the network mask as 10.10.10.1 and 255.255.255.0 respectively .

```
Ruijie(config-if)# ip address 10.10.10.1 255.255.255.0

The following example configures the default gateway address as 10.10.10.254 .
Ruijie(config-if)# ip address 10.10.10.1 255.255.255.0 gateway 10.10.10.254
```

The following example configures the master and slave IP addresses as 10.10.10.1/24 and 10.10.20.1/24 respectively.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip address 10.10.20.1 255.255.255.0
slave
```

Related Commands

Command	Description
show interface	Displays detailed information of the interface.

Platform N/A
Description

1.3 ip address negotiate

Use this command to configure an IP address for the interface through PPP negotiation. Use the **no** form of this command to restore the setting.

ip address negotiate
no ip address negotiate

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example obtains an IP address for the interface through PPP negotiation.

```
Ruijie(config)# interface dialer 1
Ruijie(onfig-if-dialer 1)# ip address negotiate
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.4 ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip broadcast-addresss *ip-address*
no ip broadcast-addresss

Parameter	Parameter	Description
Description	<i>ip-address</i>	Broadcast address of IP network

Defaults The default IP broadcast address is 255.255.255.255.

Command Mode Interface configuration mode.

Usage Guide At present, the destination address of IP broadcast packet is all "1", represented as 255.255.255.255. The RGOS software can generate broadcast packets with other IP addresses through definition, and can receive both all "1" and the broadcast packets defined by itself.

Configuration Examples The following example sets the destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip broadcast-address 0.0.0.0
```

Related	Command	Description
---------	---------	-------------

Commands	N/A	N/A
-----------------	-----	-----

Platform N/A

Description

1.5 ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter	Parameter	Description
Description	<i>access-list-number</i>	(Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all "1"), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast.

If the **no ip directed-broadcast** command is configured on an interface, RGOS will discard the directed broadcast packets received from the directly connected network.

Configuration Examples The following example enables forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip directed-broadcast
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.6 ip icmp error-interval

Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the **no** form of this command to restore the default setting.

`ip icmp error-interval DF milliseconds [bucket-size]`

no ip icmp error-interval DF milliseconds [bucket-size]

Use this command to set the rate to send other ICMP error packets. Use the **no** form of this command to restore the default setting.

`ip icmp error-interval milliseconds [bucket-size]`

no ip icmp error-interval milliseconds [bucket-siz]

Parameter	Parameter	Description
Description	<i>milliseconds</i>	The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets. The default is 100.
	<i>bucket-size</i>	The number of tokens in the bucket, in the range is from 1 to 200. The default is 10.

Defaults The default rate is 10 packets per 100 millisecond.

Command Mode Global configuration mode.

Usage Guide To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets.

If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on

ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.

It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.

Configuration Examples The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second.

```
Ruijie(config)# ip icmp error-interval DF 1000 100
```

The following example sets the rate to send other ICMP error packets to 10 per second.

```
Ruijie(config)# ip icmp error-interval 1000 10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.7 ip mask-reply

Use this command to configure the RGOS software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip mask-reply
no ip mask-reply

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Interface configuration mode.

Usage Guide Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

Configuration Examples The following example sets the FastEthernet 0/1 interface of a device to respond the ICMP mask request message.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip mask-reply
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

1.8 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip mtu bytes

no ip mtu

Parameter	Parameter	Description
Description	<i>bytes</i>	Maximum transmission unit of IP packet , in the range from 68 to 1500 bytes

Defaults It is the same as the value configured in the interface command **mtu** by default.

Command Mode Interface configuration mode.

Usage Guide If an IP packet is larger than the IP MTU, the RGOS software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.

If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

Configuration Examples The following example sets the IP MTU value of the fastEthernet 0/1 interface to 512 bytes.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip mtu 512
```

Related	Command	Description
Commands	mtu	Sets the MTU value of an interface.

Platform N/A
Description

1.9 ip redirects

Use this command to allow the RGOS software to send an ICMP redirection message in the interface

configuration mode. Use the **no** form of this command to disable this function.

ip redirects

no ip redirects

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.

Configuration Examples The following example disables ICMP redirection for the fastEthernet 0/1 interface.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# no ip redirects
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.10 ip source-route

Use this command to allow the RGOS software to process an IP packet with source route information in global configuration mode. Use the **no** form of this command to disable this function.

ip source-route

no ip source-route

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide RGOS supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded.

Configuration The following example disables the IP source route.

Examples

```
Ruijie(config)# no ip source-route
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.11 ip ttl

Use this command to set the TTL value of the unicast packet. Use the **no** form of this command to restore the default setting.

ip ttl *value*

no ip ttl

Parameter Description	Parameter	Description
	<i>value</i>	Sets the TTL value of the unicast packet, in the range from 0 to 255.

Defaults The default is 64.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example sets the TTL value of the unicast packet to 100.

Examples

```
Ruijie(config)# ip ttl 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.12 ip unnumbered

This command is used to configure unnumbered interfaces. After an interface is set to an unnumbered interface, IP can be run on the interface and packets can be sent or received on the interface. Use the **no** form of this command to restore the default setting.

ip unnumbered *interface-type interface-number*

no ip unnumbered

Parameter	Parameter	Description
Description	<i>interface-type</i>	Type of the associated interface
	<i>interface-number</i>	No. of the associated interface

Defaults No unnumbered interface is configured by default.

Command mode Interface configuration mode

Usage Guide An unnumbered interface indicates that IP is enabled on the interface but no IP address is allocated for the interface. An unnumbered interface must associate with an interface with an IP address. The source IP address of the IP packets generated on an unnumbered interface is the IP address of the associated interface. In addition, the routing protocol process determines whether to send route update packets to the unnumbered interface according to the IP address of the associated interface. Pay attention to the following when using an unnumbered interface:

An Ethernet interface cannot be set to an unnumbered interface.

When SLIP, HDLC, PPP, LAPB, and Frame-relay are encapsulated on a serial port, the port can be set to an unnumbered interface. When a frame relay is encapsulated, only a point-to-point subinterface can be set to an unnumbered interface. In the case of X.25 encapsulation, unnumbered interface is not allowed.

The **ping** command cannot be used to check whether an unnumbered interface is working properly because the interface does not have an IP address. The status of an unnumbered interface can be remotely monitored over SNMP.

The network cannot be enabled using an unnumbered interface.

Configuration Examples The following example configures the local interface as an unnumbered interface and sets the associated interface to FastEthernet 0/1 (an IP address is configured for the interface).

```
Ruijie(config)# int virtual-ppp 1
Ruijie(config-if)# ip unnumbered fastEthernet 0/1
```

Related Commands	Command	Description
	show interface	Displays the detailed information about the interface.

Platform N/A

Description

1.13 ip unreachable

Use this command to allow the RGOS software to generate ICMP destination unreachable messages. Use the **no** form of this command to disable this function.

ip unreachable

no ip unreachable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide RGOS software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upper protocol of this message.

RGOS software will send ICMP host unreachable message to source data if it can not forward a message due to no routing.

This command influences all ICMP destination unreachable messages.

Configuration Examples The following example disables sending ICMP destination unreachable message on FastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# no ip unreachable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.14 show ip interface

Use this command to display the IP status information of an interface.

show ip interface [*interface-type interface-number* | **brief**]

Parameter	Parameter	Description
Description	<i>interface-type</i>	Specifies interface type.

<i>interface-number</i>	Specifies interface number.
<i>brief</i>	Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide When an interface is available, RGOS will create a direct route in the routing table. The interface is available in that the RGOS software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the RGOS software removes the appropriate direct route from the routing table.

If the interface is unavailable, for example, two-way communication is allowed, the line protocol status will be shown as "UP". If only the physical line is available, the interface status will be shown as "UP".

The results shown may vary with the interface type, because some contents are the interface-specific options

Configuration Examples The following example displays the output of the **show ip interface brief** command.

```
Ruijie#show ip interface brief
Interface IP-Address (Pri) IP-Address (Sec) Status Protocol
GigabitEthernet 0/10 2.2.2.2/24 3.3.3.3/24 down down
GigabitEthernet 0/11 no address no address down down
VLAN 1 1.1.1.1/24 no address down down
```

Description of fields:

Field	Description
Status	Link status of an interface. The value can be up , down , or administratively down .
Protocol	IPv4 protocol status of an interface.

The following example displays the output of the **show ip interface vlan** command.

```
SwitchA#show ip interface vlan 1
VLAN 1
IP interface state is: DOWN
IP interface type is: BROADCAST
IP interface MTU is: 1500
IP address is:
1.1.1.1/24 (primary)
IP address negotiate is: OFF
Forward direct-broadcast is: OFF
ICMP mask reply is: ON
Send ICMP redirect is: ON
```

```

Send ICMP unreachable is: ON
DHCP relay is: OFF
Fast switch is: ON
Help address is:
Proxy ARP is: OFF
ARP packet input number: 0
  Request packet: 0
  Reply packet: 0
  Unknown packet: 0
TTL invalid packet number: 0
ICMP packet input number: 0
  Echo request: 0
  Echo reply: 0
  Unreachable: 0
  Source quench: 0
  Routing redirect: 0

```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface hardware status and line protocol status are "UP".
IP interface type is:	Show the interface type, such as broadcast, point-to-point, etc.
IP interface MTU is:	Show the MTU value of the interface.
IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-broadcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachable is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fast switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
ARP packet input number:	Show the total number of ARP packets received on the interface, including:
Request packet:	ARP request packet
Reply packet:	ARP reply packet
Unknown packet:	ARP reply packet

	Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: Echo request: Echo reply: Unreachable: Source quench: Routing redirect:	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet
Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

Related Commands	Command	Description
	N/A.	N/A.

Platform N/A.
Description

1.15 show ip packet queue

Use this command to display the statistics of IP packet queues.

show ip packet queue

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration The following example displays the statistics of IP packet queues.

Examples

```
Ruijie#show ip packet queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
Discards:
  Failed to alloc skb: 0.
  Receive queue overflow: 0.
```

```

Unknow protocol drops: 0.
ICMP rcv drops: 0. for skb check fail.
ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
Success: 15644
Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
It records 187 us as max time in ICMP reply process.
Failed to alloc ebuf: 0
Dropped by EFMP: 0
NoRoutes: 887
Get vrf fails: 0
Cannot assigned address drops: 0
Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.

```

Field	Description
IP packet receive queue	Statistics of received packets
Discards	Statistics of discarded packets
Sent packets	Statistics of sent packets
ICMP error queue	Statistics of ICMP error packets

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

1.16 show ip packet statistics

Use this command to display the statistics of IP packets.

show ip packet statistics [total | *interface-name*]

**Parameter
Description**

Parameter	Description
<i>interface-name</i>	Interface name
<i>total</i>	Displays the total statistics of all interfaces.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration

The following example displays the output of this command.

Examples

```
Ruijie# show ip packet statistics
Total
Received 1000 packets, 1000000 bytes
Unicast:1000,Multicast:0,Broadcast:0
Discards:0
HdrErrors:0 (BadChecksum:0,TTLExceeded:0,Others:0)
NoRoutes:0
Others:0
Sent 100 packets, 6000 bytes
Unicast:50,Multicast:50,Broadcast:0

VLAN 1
Received 1000 packets, 1000000 bytes
Unicast:1000,Multicast:0,Broadcast:0
Discards:0
HdrErrors:0 (BadChecksum:0,TTLExceeded:0,Others:0)
NoRoutes:0
Others:0
Sent 100 packets, 6000 bytes
Unicast:50,Multicast:50,Broadcast:0
```

**Related
Commands**

Command	Description
ip default-gateway	Configures the default gateway, which is only supported on the Layer 2 switch.

**Platform
Description**

N/A

1.17 show ip raw-socket

Use this command to display IPv4 raw sockets.

show ip raw-socket [*num*]

**Parameter
Description**

Parameter	Description
<i>num</i>	Protocol.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration

The following example displays all IPv4 raw sockets.

Examples

```
Ruijie# show ip raw-socket
```

```

Number Protocol Process name
1      ICMP      dhcp.elf
2      ICMP      vrrp.elf
3      IGMP      igmp.elf
4      VRRP      vrrp.elf
Total: 4

```

Field Description

Field	Description
Number	Number
Protocol	Protocol
Process name	Process name
Total	Total number

Related
Commands

Command	Description
N/A	N/A

Platform
Description

N/A

1.18 show ip sockets

Use this command to display all IPv4 sockets.

show ip sockets

Parameter
Description

Parameter	Description
N/A.	N/A.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration

The following displays all IPv4 sockets.

Examples

```

Ruijie# show ip sockets
Number Process name      Type      Protocol LocalIP:Port  ForeignIP:Port
State
1      dhcp.elf              RAW      ICMP      0.0.0.0:1     0.0.0.0:0
*
2      vrrp.elf              RAW      ICMP      0.0.0.0:1     0.0.0.0:0
*
3      igmp.elf              RAW      IGMP      0.0.0.0:2     0.0.0.0:0

```

```

*
4      vrrp.elf      RAW      VRRP      0.0.0.0:112      0.0.0.0:0
*
5      dhcpc.elf    DGRAM    UDP      0.0.0.0:68      0.0.0.0:0
*
6      rg-snmpd     DGRAM    UDP      0.0.0.0:161     0.0.0.0:0
*
7      wbav2        DGRAM    UDP      0.0.0.0:2000    0.0.0.0:0
*
8      vrrp_plus.elf DGRAM    UDP      0.0.0.0:3333    0.0.0.0:0
*
9      mpls.elf     DGRAM    UDP      0.0.0.0:3503    0.0.0.0:0
*
10     rds_other_th DGRAM    UDP      0.0.0.0:3799    0.0.0.0:0
*
11     rg-snmpd     DGRAM    UDP      0.0.0.0:14800   0.0.0.0:0
*
12     rg-sshd     STREAM   TCP      0.0.0.0:22      0.0.0.0:0
LISTEN
13     rg-telnetd   STREAM   TCP      0.0.0.0:23      0.0.0.0:0
LISTEN
14     wbard        STREAM   TCP      0.0.0.0:4389    0.0.0.0:0
LISTEN
15     wbard        STREAM   TCP      0.0.0.0:7165    0.0.0.0:0
LISTEN
Total: 15
    
```

Field Description

Field	Description
Number	Serial number.
Process name	Process name.
Type	Socket type, including the following types: RAW: raw sockets DGRAM: datagram type STREAM: stream type.
Protocol	Protocol.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	Peer IP address and port.
State	State. This field is for only TCP sockets.
Total	The total number of sockets.

Related
Commands

Command	Description
N/A	N/A

Platform N/A
Description

1.19 show ip udp

Use this command to display IPv4 UDP sockets.

show ip udp [local-port num]

Use this command to display IPv4 UDP socket statistics.

show ip udp statistics

Parameter	Parameter	Description
Description	local-port num	Local port number

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration The following example displays all IPv4 UDP sockets.

Examples

```
Ruijie# show ip udp
```

Number	Local Address	Peer Address	Process name
1	0.0.0.0:68	0.0.0.0:0	dhcpc.elf
2	0.0.0.0:161	0.0.0.0:0	rg-snmpd
3	0.0.0.0:2000	0.0.0.0:0	wbav2
4	0.0.0.0:3333	0.0.0.0:0	vrrp_plus.elf
5	0.0.0.0:3503	0.0.0.0:0	mpls.elf
6	0.0.0.0:3799	0.0.0.0:0	rds_other_th
7	0.0.0.0:14800	0.0.0.0:0	rg-snmpd

Field Description

Field	Description
Number	Number.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2 ARP Commands

2.1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. Use the **no** form of this command to restore the default setting.

arp [*vrf name*] *ip-address mac-address type*

no arp [*vrf name*] *ip-address*

Parameter	Parameter	Description
Description	<i>vrf name</i>	The name of VRF instance.
	<i>ip-address</i>	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
	<i>mac-address</i>	48-bit data link layer address
	<i>type</i>	ARP encapsulation type. The keyword is arpa for the Ethernet interface.

Defaults There is no static mapping record in the ARP cache table by default.

Command Mode Global configuration mode.

Usage Guide RGOS finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table. Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The **clear arp-cache** command can be used to delete the ARP mapping that is learned dynamically.

Configuration Examples The following example sets an ARP static mapping record for a host in the Ethernet.

```
Ruijie(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

Related Commands	Command	Description
	clear arp-cache	Clears the ARP cache table

Platform Description N/A

2.2 arp anti-ip-attack

Use the **arp anti-ip-attack** command to set the parameter or disable this function. Use the **no** form of this command to restore the default setting.

arp anti-ip-attack *num*

no arp anti-ip-attack

Parameter	Parameter	Description
Description	<i>num</i>	The number of the IP message to trigger the ARP to set the discarded entry in the range from 0 to 100. 0 stands for disabling the arp anti-ip-attack function.

Defaults By default, set the discarded entry after 3 unknown unicast messages are sent to the CPU.

Command Mode Global configuration mode.

Usage Guide For the messages corresponds to the directly-connected route, if the switch does not learn the ARP that corresponds to the destination IP address, it is not able to forward the message in hardware, and it needs to send the message to the CPU to resolve the address(that is the ARP learning). Sending large number of this message to the CPU will influence the other tasks of the switch. To prevent the IP messages from attacking the CPU, a discarded entry is set to the hardware during the address resolution, so that all sequential messages with that destination IP address are not sent to the CPU. After the address resolution, the entry is updated to the forwarding status, so that the switch could forward the message with that destination IP address in hardware.

In general, during the ARP request ,if the switch CPU receives three destination IP address messages corresponding to the ARP entry, it is considered to be possible to attack the CPU and the switch sets the discarded entry to prevent the unknown unicast message from attacking the CPU. User could set the *num* parameter of this command to decide whether it attacks the CPU in specific network environment or disable this function.

The arp anti-ip-attack function needs to occupy the switch hardware routing resources when attacked by the unknown unicast message. If there are enough resources, the **arp anti-ip-attack *num*** could be smaller. If not, in order to preferential ensure the use of the normal routing, the *num* could be larger or disable this function.

Configuration Examples The following example sets the IP message number that triggers to set the discarding entry as 5.

```
Ruijie(config)# arp anti-ip-attack 5
```

The following example disables the ARP anti-ip-attack function.

```
Ruijie(config)# arp anti-ip-attack 0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.3 arp cache interface-limit

Use this command to set the maximum number of ARP learned on the interface.

Use the **no** form of this command to restore the default setting.

arp cache interface-limit *limit*

no arp cache interface-limit

Parameter	Parameter	Description
Description	<i>limit</i>	Sets the maximum number of ARP learned on the interface, including static and dynamic ARPs, in the range from 0 to the number supported on the interface. 0 indicates that the number is not limited.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide This function can prevent ARP attacks from generating ARP entries to consume memory. *limit* must be no smaller than the number of ARPs learned on the interface. Otherwise, the configuration does not take effect.

Configuration Examples The following example sets the maximum number of ARP learned on the interface to 300.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp cache interface-limit 300
```

The following example restores the default setting.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp any-ip
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.4 arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface. Use the **no** form of this command to restore the default setting.

arp gratuitous-send interval *seconds* [*number*]

no arp gratuitous-send

Parameter	Parameter	Description
Description	<i>seconds</i>	The time interval to send the free ARP request message in the range from 1 to 3,600 in the unit of seconds.
	<i>number</i>	The number of free ARP request message to be sent in the range from 1 to 100 with 1 being the default value.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

Configuration Examples The following example sets to send one free ARP request to SVI 1 per second.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# arp gratuitous-send interval 1
```

The following example stops sending the free ARP request to SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# no arp gratuitous-send
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.5 arp oob

Use this command to configure the static ARP on the management interface. Use the **no** form of this command to restore the default setting.

arp oob [*mgmt.-name*] *ip-address mac-address type*

no arp oob [*mgmt.-name*] *ip-address*

Parameter	Parameter	Description
Description	<i>ip-address</i>	The IP address corresponding to the MAC address, written as four groups of dotted decimal values.
	<i>mac-address</i>	The data link layer address, composed of 48 bits.
	<i>type</i>	The ARP encapsulation type. The key word for the Ethernet interface is arpa .
	<i>mgmt.-name</i>	Specifies the ARP-mapping management interface when there are multiple management interfaces.

Defaults No static ARP is configured by default.

Command Mode Global configuration mode

Usage Guide RGOS uses the ARP cache table to search for the 48-bit MAC address according to the 32-bit IP address.

Most hosts support dynamic ARP analysis, so static ARP mapping does not need to be configured. The clear arp-cache oob command is used to clear the ARP mapping learned by the management port dynamically.

If no management interface is specified, the static ARP is configured on the first management interface by default. If you specify the first management interface, the *mgmt-name* parameter is not displayed by running the **show run** command.

Configuration Examples The following example configures a static ARP mapping record for the Ethernet host

```
Ruijie(config)# arp oob 1.1.1.1 4e54.3800.0002 arpa
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.6 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. Use the **no** form of this command to restore the default setting.

arp retry interval *seconds*

no arp retry interval

Parameter Description	Parameter	Description
	<i>seconds</i>	Time for retransmitting the ARP request message in the range from 1 to 3600 in the unit of seconds.

Defaults The default is 1.

Command Mode Global configuration mode.

Usage Guide The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

Configuration The following example sets the retry interval of the ARP request as 30 seconds.

Examples Ruijie(config)# arp retry interval 30

Related	Command	Description
Commands	arp retry times	Number of times for retransmitting an ARP request message.

Platform N/A

Description

2.7 arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. Use the **no** form of this command to restore the default setting.

arp retry times *number*

no arp retry times

Parameter	Parameter	Description
Description	<i>number</i>	The times of sending the same ARP request in the range from 1 to100.When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent.

Defaults The default is 5.

Command Global configuration mode.

Mode

Usage Guide The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

Configuration The following example sets the local ARP request not to be retried.

Examples Ruijie(config)# arp retry times 1

The following example sets the local ARP request to be retried for one time.

Ruijie(config)# arp retry times 2

Related	Command	Description
Commands	arp retry interval	Interval for retransmitting an ARP request message

Platform N/A

Description

2.8 arp suppress-auth-vlan-req

Use this command to disable the SVI interface from sending the ARP request to the authentication VLAN. Use the **no** form of this command to disable this function.

arp suppress-auth-vlan-req

no arp suppress-auth-vlan-req

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide In gateway authentication mode, all sub-VLANs of SuperVLAN are authentication VLANs by default. Users on authentication VLANs should pass the authentication before accessing the network. Static ARP table entries are generated on the device after users pass authentication. The device does not need to send ARP requests to the authentication VLAN when accessing these users. If the device accesses users on the authentication-exemption VLAN, it only needs to send ARP requests to the authentication-exemption VLAN.

In gateway authentication mode, the device enables suppression of ARP request sent to the authentication VLAN by default. If the device needs to access authentication-exemption users on the authentication VLAN, this function should be disabled.

Configuration Examples The following example disables VLAN 2 from sending the ARP request to the authentication VLAN.

```
Ruijie(config)# interface vlan 2
Ruijie(config-if-VLAN 2)# arp suppress-auth-vlan-req
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.9 arp proxy-resolved

Use this command to enable a device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as an ARP proxy. Use the **no** form of this command to disable this function.

arp proxy-resolved

no arp proxy-resolved

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	<p>After the arp proxy-resolved command is configured, the active VRRP device first judges, upon receiving an ARP request, whether the ARP entry corresponding to the destination IP address exists. If yes, the active VRRP device acts as an ARP proxy. If no, the active VRRP device does not act as an ARP proxy. In addition, the gateway automatically requests the ARP entry corresponding to the destination IP address in broadcast mode. This prevents a case that the gateway fails to act as a proxy to respond to an ARP request of the destination IP address due to absence of the ARP entry corresponding to the destination IP address.</p> <p>After the no arp proxy-resolved command is configured, if the proxy conditions are met, the active VRRP device directly acts as a proxy upon receiving an ARP request, with no need to judge whether the ARP entry corresponding to the destination IP address has been resolved.</p>	
Configuration Examples	<p>The following example disables a device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as an ARP proxy.</p> <pre>Ruijie(config)# no arp proxy-resolved</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.10 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache.

Use the **no** form of this command to restore the default setting.

arp timeout *seconds*

no arp timeout

Parameter	Parameter	Description
Description	<i>secondsv</i>	The timeout is in the range from 0 to 2147483 in the unit of seconds.
Defaults	The default is 3600.	
Command	Interface configuration mode/Global configuration mode	

Mode

Usage Guide The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

Configuration Examples The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet port 0/1 to 120 seconds.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# arp timeout 120
```

Related Commands

Command	Description
clear arp-cache	Clears the ARP cache list.
show interface	Displays the interface information.

Platform N/A
Description

2.11 arp trusted

Use this command to set the maximum number of trusted ARP entries. Use the **no** form of this command to restore the default setting.

arp trusted *number*
no arp trusted

Parameter Description

Parameter	Description
<i>number</i>	Maximum number of trusted ARP entries.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide To make this command valid, enable the trusted ARP function firstly. The trusted ARP entries and other entries share the memory. Too much trusted ARP entries may lead to insufficient ARP entry space. In general, you should set the maximum number of trusted ARP entries according to your real requirements.

Configuration Examples The following example sets 1000 trusted ARPs.

```
Ruijie(config)# arp trusted 1000
```

Related Commands	Command	Description
	service trustedarp	Enables the trusted ARP function.

Platform N/A
Description

2.12 arp trusted aging

Use this command to set trusted ARP aging. Use the **no** form of this command to restore the default setting.

arp trusted aging

no arp trusted aging

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Use this command to set trusted ARP aging. Aging time is the same as dynamic ARP aging time. Use the **arp timeout** command to set aging time in interface mode.

Configuration Examples N/A

Related Commands	Command	Description
	service trustedarp	Enables trusted ARP function.

Platform N/A
Description

2.13 arp trusted user-vlan

Use this command to execute the VLAN transformation while setting the trusted ARP entries. Use the **no** form of this command to restore the default setting.

arp trusted user-vlan vid1 translated-vlan vid2

no arp trusted user-vlan vid1 translated-vlan vid2

Parameter Description	Parameter	Description
	<i>vid1</i>	VID set by the server.
	<i>vid2</i>	VID after the transformation.

Defaults	This function is disabled by default.				
Command Mode	Global configuration mode.				
Usage Guide	In order to validate this command, enable the trusted ARP function first. This command is needed only when the VLAN sent by the server is different from the VLAN which takes effect in the trusted ARP entry.				
Configuration Examples	The following example sets the VLAN sent by the server to 3, but the VLAN which takes effect in the trusted ARP entry to 5. <pre>Ruijie(config)# arp trusted user-vlan 3 translated-vlan 5</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>service trustedarp</td> <td>Enables the trusted ARP function.</td> </tr> </tbody> </table>	Command	Description	service trustedarp	Enables the trusted ARP function.
Command	Description				
service trustedarp	Enables the trusted ARP function.				
Platform Description	N/A				

2.14 arp trust-monitor enable

Use this command to enable egress gateway trusted ARP. Use the **no** form of this command to restore the default setting.

arp trust-monitor enable

no arp trust-monitor enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults	This function is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	<p>This command is used to enable anti-ARP spoofing to prevent excessive useless ARP entries from occupying device resources. After ARP trustworthiness detection is enabled on a Layer-3 interface, the device receives ARP request packets from this interface:</p> <ol style="list-style-type: none"> 1. If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs NUD after 1 to 5 seconds. That is, the device begins to age the newly learned ARP entry and sends a unicast ARP request. If the device receives an ARP update packet from the peer end within the aging time, it stores the entry. If not, it deletes the entry. 2. If the corresponding ARP entry exists, NUD is not performed. 3. If the MAC address in the existing dynamic ARP entry is updated, the device also performs

NUD.

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

After this function is disabled, NUD is not required for learning and updating ARP entries.

Configuration The following example enables egress gateway trusted ARP.

Examples

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp trust-monitor enable
```

The following example disables egress gateway trusted ARP.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

2.15 arp unresolve

Use this command to set the maximum number of the unresolved ARP entries. Use **no** form of this command to restore the default setting.

arp unresolve *number*

no arp unresolve

Parameter	Parameter	Description
Description	<i>number</i>	The maximum number of the unresolved ARP entries in the range from 1 to the ARP table size supported by the device.

Defaults The default is the ARP table size supported by the device.

Command Mode Global configuration mode.

Usage Guide If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

Configuration The following example sets the maximum number of the unresolved items to 500.

Examples

```
Ruijie(config)# arp unresolve 500
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

2.16 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table.

clear arp-cache [*vrf vrf_name* | **trusted**] [*ip [mask]*] | **interface** *interface-name*]

Parameter	Parameter	Description
Description	<i>trusted</i>	Deletes trusted ARP entries. Dynamic ARP entries are deleted by default.
	<i>vrf vrf_name</i>	Deletes dynamic ARP entries of the specified VRF instance. The default is the public instance.
	<i>ip</i>	Deletes ARP entries of the specified IP address. If <i>trusted</i> value is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
	<i>mask</i>	Deletes ARP entries in a subnet mask. If <i>trusted</i> value is specified, trusted ARP entries in the subnet mask are deleted; otherwise, all dynamic ARP entries are deleted. The dynamic ARP entry specified by the IP address is deleted by default.
	interface <i>interface-name</i>	Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide On a NFPP-based (Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two **clear arp** times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.

Configuration Examples The following example deletes all dynamic ARP mapping records.

```
Ruijie# clear arp-cache
```

The following deletes the dynamic ARP entry 1.1.1.1.

```
Ruijie# clear arp-cache 1.1.1.1
```

The following example deletes the dynamic ARP entry on interface SV11.

```
Ruijie# clear arp-cache interface Vlan 1
```

Related	Command	Description
---------	---------	-------------

Commands	arp	Adds a static mapping record to the ARP cache table.
-----------------	------------	--

Platform N/A

Description

2.17 clear arp-cache oob

Use this command to clear dynamic ARP mapping records.

clear arp-cache oob [*ip* [*mask*]]

Parameter	Parameter	Description
Description	<i>ip</i>	Clears the ARP table entry of the specified IP address. All dynamic ARP table entries are cleared by default.
	<i>mask</i>	Clears the ARP table entry within the specified subnet. The dynamic ARP table entry of the specified IP address (the previous parameter) is cleared by default.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide On a device supporting Network Foundation Protection Policy (NFPP), every MAC / IP address receives an ARP packet per second by default. If the **clear arp oob** command is run twice within one second, the second response packet may be filtered, causing ARP uanalysis for a short time.

Configuration The following example clears the cache table of dynamic ARP mapping records.

Examples Ruijie# clear arp-cache oob

The following example clears dynamic ARP table entry 1.1.1.1.

Ruijie# clear arp-cache oob 1.1.1.1

The following example clears the dynamic ARP table entry within the specified subnet.

Ruijie# clear arp-cache oob 1.0.0.0 255.0.0.0

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

2.18 ip proxy-arp

Use this command to enable ARP proxy function on the interface. Use the **no** form of this command to restore the default setting.

ip proxy-arp
no ip proxy-arp

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

Configuration Examples The following example enables ARP on FastEthernet port 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip proxy-arp
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.19 local-proxy-arp

Use this command to enable local proxy ARP on the SVI interface. Use the **no** form of this command to restore the default setting.

local-proxy-arp
no local-proxy-arp

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide With local proxy ARP enabled, the device helps a host to obtain MAC addresses of other hosts on the subnet. If the device enables switchport protected, users on different ports are segregated on

layer 2. After local proxy ARP is enabled, the device serves as a proxy to send a response after receiving an ARP request. The ARP response contains a MAC address which is the device's Ethernet MAC address, realizing communication between different hosts through L3 routes.

Configuration The following example enables local proxy ARP on VLAN1.

Examples

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# local-proxy-arp
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.20 service trustedarp

Use this command to enable the trusted ARP function. Use the **no** form of this command to restore the default setting.

service trustedarp

no service trustedarp

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

**Command
Mode** Global configuration mode

Usage Guide The trusted ARP function of the device is to prevent the ARP fraud function. As a part of the GSN scheme, it should be used together with the GSN scheme.

Configuration The following example enables the trusted ARP function in global configuration mode.

Examples

```
config
service trustedarp
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.21 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

show arp [*interface-type interface-number* | **trusted** [*ip [mask]*] | [**vrf vrf-name**] [*ip [mask]*] | *mac-address* | **static** | **complete** | **incomplete**]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	Displays the ARP entry of a specified Layer-2 or Layer-3 port.
	vrf <i>vrf_name</i>	VRF instance, which Displays the ARP entry with specified VRF.
	trusted	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
	<i>ip</i>	Displays the ARP entry of the specified IP address. If trusted is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
	<i>mask</i>	Displays the ARP entries of the network segment included within the mask. If trusted is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
	static	Displays all the static ARP entries.
	complete	Displays all the resolved dynamic ARP entries.
	incomplete	Displays all the unresolved dynamic ARP entries.
	<i>mac-address</i>	Displays the ARP entry with the specified mac address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the output result of the **show arp** command:

```
Ruijie# show arp
Total Numbers of Arp: 7
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1
Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1
Internet 192.168.195.65 0 0018.8b7b.713e arpa VLAN 1
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.63 0 001a.a0b5.3990 arpa VLAN 1
Internet 192.168.195.62 0 001a.a0b5.0b25 arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses
Interface	Interface associated with the IP addresses

The following example displays the output result of `show arp 192.168.195.68`

```
Ruijie# show arp 192.168.195.68
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 1 0013.20a5.7a5f arpa VLAN 1
```

The following example displays the output result of `show arp 192.168.195.0 255.255.255.0`

```
Ruijie# show arp 192.168.195.0 255.255.255.0
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.2 1 00d0.f8ff.f00e arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
Internet 192.168.195.1 0 00d0.f8a6.5af7 arpa VLAN 1
Internet 192.168.195.51 1 0018.8b82.8691 arpa VLAN 1
```

The following example displays the output result of `show arp 001a.a0b5.378d`

```
Ruijie# show arp 001a.a0b5.378d
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.67 4 001a.a0b5.378d arpa VLAN 1
```

The following example displays the output result of `show arp static`

```
Ruijie# show arp static
Protocol Address Age(min) Hardware Type Interface Origin
Internet 192.168.23.55 <static> 0000.0000.0010 arpa VLAN 100
Configure
Internet 192.168.23.56 <static> 0000.0000.0020 arpa VLAN 100
Authentication
Internet 192.168.23.57 <static> 0000.0000.0020 arpa VLAN 100
DHCP-Snooping
2 static arp entries exist.
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

2.22 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

show arp counter

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the output result of the **show arp counter** command:

Examples

```
Ruijie#sho arp counter
ARP Limit:                75000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1 incomplete: 0)
Total:                    1
```

The meaning of each field in the ARP cache table is described in the following Table.

Parameter	Description
overlay	Indicates the number of VxLAN-related ARP entries.
underlayer	Indicates the number of VxLAN-irrelated ARP entries.

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

2.23 show arp detail

Use this command to display the details of the Address Resolution Protocol (ARP) cache table.

show arp detail [*interface-type interface-number* | **trusted** [*ip [mask]*] | [**vrf** *vrf-name*] [*ip [mask]*]

| *mac-address* | **static** | **complete** | **incomplete**] | **subvlan** { *subvlan-number* | **min-max** *min_value* *max_value*]

Parameter Description

Parameter	Description
<i>interface-type interface-number</i>	Displays the ARP of the layer 2 port or the layer 3 interface.
vrf <i>vrf_name</i>	VRF instance, which Displays the ARP entry with specified VRF.
<i>trusted</i>	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
<i>ip</i>	Displays the ARP entry of the specified IP address.
<i>ip mask</i>	Displays the ARP entries of the network segment included within the mask.
<i>mac-address</i>	Displays the ARP entry of the specified MAC address.
<i>static</i>	Displays all the static ARP entries.
<i>completev</i>	Displays all the resolved dynamic ARP entries.
<i>incomplete</i>	Displays all the unresolved dynamic ARP entries.
subvlan	Displays the ARP entries of the specified subvlan
<i>subvlan-number</i>	Subvlan ID
min-max	Displays the minimum and maximum subvlan ID
<i>min_value</i>	Minimum subvlan ID
<i>max_value</i>]	Maximum subvlan ID.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the ARP details, such as the ARP type (Dynamic, Static, Local, Trust), the information on the layer2 port.

If you enter a *min_value* greater than *max_value*, no error message is prompted. Instead, ARP entries corresponding to the subvlan are displayed.

Configuration Examples The following example displays the output result of the **show arp detail** command:

```
Ruijie# show arp detail
IP Address      MAC Address      Type      Age (min)  Interface  Port
SubVlan
20.1.1.2        0020.0101.0002   Static    --         Te2/5      --    --
20.1.1.1        00d0.f822.33bb   Local     --         Te2/5      --    --
1.1.1.2         00d0.1111.1112   Dynamic   1          V12        Te2/1  4
1.1.1.1         00d0.f822.33bb   Local     --         V12        --    --
```

The following example displays arp details including InnerVLAN on products supporting QinQ termination:

```
Ruijie# show arp detail
IP Address      MAC Address      Type      Age (min)  Interface  Port
SubVlan  InnerVlan
20.1.1.2      0020.0101.0002  Static    --         Te2/5      --    --
20.1.1.1      00d0.f822.33bb  Local     --         Te2/5      --    --
1.1.1.2       00d0.1111.1112  Dynamic   1          V12        Te2/1  4
300
1.1.1.1       00d0.f822.33bb  Local     --         V12        --    --
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
IP Address	IP address corresponding to the hardware address
MAC Address	hardware address corresponding to the IP address
Age (min)	Age of the ARP learning, in minutes
Port	Layer2 port associated with the ARP
Type	ARP type, includes the Static, Dynamic, Trust,Local
Interface	Layer 3 interface associated with the IP addresses
SubVLAN	SubVLAN corresponding to the ARP entries
InnerVLAN	InnerVLAN or CE-VLAN corresponding to the ARP entries
Subvni	Vni corresponding to the ARP entries, namely ID of the VxLAN.
Location	Local: ARP entries are generated or learned on the local device. Remote: ARP entries are synced from a remote gateway.

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.24 show arp oob

Use this command to display the ARP cache table.

show arp oob [*ip* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]

**Parameter
Description**

Parameter	Description
<i>ip</i>	Displays ARP table entries of the specified IP address.
<i>mask</i>	Displays ARP table entries within the IP subnet.
static	Displays all static ARP table entries.

complete	Displays all analyzed ARP table entries.
incomplete	Displays all unanalyzed ARP table entries.
<i>mac-address</i>	Displays ARP table entries of the specified MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the ARP cache table. The **complete** / **incomplete** key word represents analyzed / unanalyzed ARP table entries.

Configuration Examples The following example displays the outcome of the running the show arp oob command.

```
Ruijie# show arp oob
Total Numbers of Arp: 7
Protocol  Address          Age (min)  Hardware          Type  Interface
Internet  192.168.195.68    0          0013.20a5.7a5f   arpa  mgmt 0
Internet  192.168.195.67    0          001a.a0b5.378d   arpa  mgmt 0
Internet  192.168.195.65    0          0018.8b7b.713e   arpa  mgmt 0
Internet  192.168.195.64    0          0018.8b7b.9106   arpa  mgmt 0
Internet  192.168.195.63    0          001a.a0b5.3990   arpa  mgmt 0
Internet  192.168.195.62    0          001a.a0b5.0b25   arpa  mgmt 0
Internet  192.168.195.5     --         00d0.f822.33b1   arpa  mgmt 0
```

The following example displays the outcome of running the **show arp oob 192.168.195.68** command.

```
Ruijie# show arp oob 192.168.195.68
Protocol  Address          Age (min)  Hardware          Type  Interface
Internet  192.168.195.68    1          0013.20a5.7a5f   arpa  mgmt 0
```

The following example displays the outcome of running the **show arp oob 192.168.195.0 255.255.255.0**.

```
Ruijie# show arp 192.168.195.0 255.255.255.0
Protocol  Address          Age (min)  Hardware          Type  Interface
Internet  192.168.195.64    0          0018.8b7b.9106   arpa  mgmt 0
Internet  192.168.195.2     1          00d0.f8ff.f00e   arpa  mgmt 0
Internet  192.168.195.5     --         00d0.f822.33b1   arpa  mgmt 0
Internet  192.168.195.1     0          00d0.f8a6.5af7   arpa  mgmt 0
Internet  192.168.195.51    1          0018.8b82.8691   arpa  mgmt 0
```

The following example displays the outcome of running the **show arp oob 001a.a0b5.378d** command.

```
Ruijie# show arp 001a.a0b5.378d
Protocol  Address          Age (min)  Hardware          Type  Interface
Internet  192.168.195.67    4          001a.a0b5.378d   arpa  mgmt 0
```

Field	Description
-------	-------------

Protocol	Only "Internet" is available at present, which indicates the IP protocol.
Address	The IPv4 address.
Age(min)	The age of the table entry. For the local IP address, the field is displayed as '-'. For the static table entry, the field is displayed as <static>. For the dynamic table entry, the field indicates the time for which the table entry has been learned, in the unit of minutes.
Hardware	48-bit MAC address, written as a dotted triple of four-digit hexadecimal numbers.
Type	Only "arpa" is available at present.
Interface	The L3 interface corresponding to the ARP table entry. The field is NULL for static ARP table entries for the IP address of the static ARP is not within any network segment directly connected with the device.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.25 show arp packet statistics

Use this command to display the statistics of ARP packets.

show arp packet statistics [*interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Displays the statistics of ARP packets on the specified interface.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays the output information of the command.

```
Ruijie# show arp packet statistics
Interface Received Received Received Sent Sent
Name Requests Replies Others Requests Replies
-----
VLAN 1 10 20 1 50 10
```



```
VLAN 2 5 8 0 10 10
VLAN 3 20 5 0 15 12
VLAN 4 5 8 0 10 10
VLAN 5 20 5 0 15 12
VLAN 6 20 5 0 15 12
VLAN 7 20 5 0 15 12
VLAN 8 5 8 0 10 10
VLAN 9 20 5 0 15 12
VLAN 10 20 5 0 15 12
VLAN 11 20 5 0 15 12
VLAN 12 20 5 0 15 12
```

Description of fields:

Field	description
Received Requests	Number of received ARP requests
Received Replies	Number of received ARP response messages
Received Others	Number of other received ARP packets
Sent Requests	Number of sent ARP requests
Sent Replies	Number of sent ARP requests

**Related
Commands**

Command	Description
N/A.	N/A.

**Platform
Description**

N/A

2.26 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the interface.

show arp timeout

**Parameter
Description**

Parameter	Description
N/A.	N/A.

Defaults

N/A.

**Command
Mode**

Privileged EXEC mode

Usage Guide

N/A.

Configuration The following example displays the output of the **show arp timeout** command:

Examples

```
Ruijie# show arp timeout
Interface arp timeout(sec)
```

```
-----
VLAN 1 3600
```

The meaning of each field in the ARP cache table is described in Table 1.

Related Commands	Command	Description
	N/A.	N/A.

Platform N/A
Description

2.27 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

show ip arp [*vrf vrf-name*]

Parameter	Parameter	Description
Description	<i>vrf-name</i>	Specifies a VRF instance.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration The following example displays the output of **show ip arp**:

Examples

```
Ruijie# show ip arp
Protocol Address Age (min) Hardware Type Interface
Internet 192.168.7.233 23 0007.e9d9.0488 ARPA FastEthernet 0/0
Internet 192.168.7.112 10 0050.eb08.6617 ARPA FastEthernet 0/0
Internet 192.168.7.79 12 00d0.f808.3d5c ARPA FastEthernet 0/0
Internet 192.168.7.1 50 00d0.f84e.1c7f ARPA FastEthernet 0/0
Internet 192.168.7.215 36 00d0.f80d.1090 ARPA FastEthernet 0/0
Internet 192.168.7.127 0 0060.97bd.ebee ARPA FastEthernet 0/0
Internet 192.168.7.195 57 0060.97bd.ef2d ARPA FastEthernet 0/0
Internet 192.168.7.183 -- 00d0.f8fb.108b ARPA FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".

Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

Related Commands	Command	Description
	N/A.	N/A.

Platform N/A
Description

3 IPv6 Commands

3.1 clear ipv6 neighbors

Use this command to clear the dynamic IPv6 neighbors.

clear ipv6 neighbors [**vrf** *vrf-name*] [**oob**] [*interface-id*]

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name. All global IPv6 neighbors are cleared without specified VRF name by default.
	oob	Clears the dynamic IPv6 neighbors discovered by neighbors on MGMT interface.
	<i>interface-id</i>	Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface.

Defaults N/A

Command Privileged EXEC mode.

Mode

Usage Guide This command does not clear all the dynamic neighbors on authentication VLAN. Note that the static neighbors will not be cleared.

Configuration The following example clears the dynamic IPv6 neighbors.

Examples

```
Ruijie# clear ipv6 neighbors
```

The following example clears the dynamic IPv6 neighbors discovered by neighbors on MGMT interface.

```
Ruijie# clear ipv6 neighbors oob
```

The following example clears the dynamically learned IPv6 neighbors on the interface gigabitEthernet 0/1.

```
Ruijie# clear ipv6 neighbors gigabitEthernet 0/1
```

Related	Command	Description
Commands	ipv6 neighbor	Configures the neighbor.
	show ipv6 neighbors	Displays the neighbor information.

Platform N/A

Description

3.2 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to restore the default setting.

ipv6 address ipv6-address/prefix-length

ipv6 address *ipv6-prefix/prefix-length eui-64*

ipv6 address *prefix-name sub-bits/prefix-length [eui-64]*

no ipv6 address

no ipv6 address *ipv6-address/prefix-length*

no ipv6 address *ipv6-prefix/prefix-length eui-64*

no ipv6 address *prefix-name sub-bits/prefix-length [eui-64]*

Parameter	Parameter	Description
Description	<i>ipv6-prefix</i>	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>ipv6-address</i>	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>prefix-length</i>	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128.
	<i>prefix-name</i>	The general prefix name. Use the specified general prefix to generate the interface address.
	<i>sub-bits</i>	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
	<i>eui-64</i>	The generated IPV6 address consists of the address prefix and the 64 bit interface ID

Defaults N/A

Command Interface configuration mode

Mode

Usage Guide When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.

The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.

If no deleted address is specified when using **no ipv6 address**, all the manually configured

addresses will be deleted.

no ipv6 address ipv6-prefix/prefix-length **eui-64** can be used to delete the addresses configured with **ipv6 address** ipv6-prefix/prefix-length **eui-64**.

```

Configuration Ruijie(config-if)# ipv6 address 2001:1::1/64
Examples      Ruijie(config-if)# no ipv6 address 2001:1::1/64
                  Ruijie(config-if)# ipv6 address 2002:1::1/64 eui-64
                  Ruijie(config-if)# no ipv6 address 2002:1::1/64 eui-64
    
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.3 ipv6 address autoconfig

Use this command to automatically configure an IPv6 stateless address for a network interface. Use the no form of this command to restore the default setting.

ipv6 address autoconfig [default]
no ipv6 address autoconfig

Parameter	Parameter	Description
Description	default	(Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the default keyword

Defaults N/A

Command Mode Interface configuration mode

Usage Guide The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address.

If the RA message contains the flag of the “other configurations”, the interface will obtain these “other configurations” through the DHCPv6. The “other configurations” usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc.

Use the **no ipv6 address autoconfig** command to delete the IPv6 address.

```

Configuration Ruijie(config-if)# ipv6 address autoconfig default
Examples      Ruijie(config-if)# no ipv6 address autoconfig
    
```

Related	Command	Description
---------	---------	-------------

Commands	ipv6 address ipv6-prefix/prefix-length [eui-64]	Configures the IPv6 address for the interface manually.
-----------------	--	---

Platform N/A

Description

3.4 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the no form of this command to restore the default setting.

ipv6 enable


no ipv6 enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.

 If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.

If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface. In this case, IPv6 cannot be disabled even when you run the **no ipv6 enable** command.

Configuration Examples Ruijie(config-if)# **ipv6 enable**

Related Commands	Command	Description
	show ipv6 interface	Displays the related information of an interface.

Platform N/A

Description

3.5 Ipv6 gateway

Use this command to configure the default gateway IPv6 address on the management port.

ipv6 gateway ipv6-address

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Configures the default gateway IPv6 address.
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	The management port is MGMT in type and 0 in ID.	
Configuration Examples	The following example configures the default gateway IPv6 address on the management port.	
Examples	<pre>Ruijie(config)# interface mgmt 0 Ruijie(config-int)# ipv6 gateway 2001:1::1 Ruijie(config-int)# exit Ruijie(config)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.6 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

ipv6 general-prefix prefix-name ipv6-prefix/prefix-length
no ipv6 general-prefix prefix-name ipv6-prefix/prefix-length

Parameter	Parameter	Description
Description	<i>prefix-name</i>	The general prefix name.
	<i>pv6-prefix</i>	The network prefix value of the general-prefix following the format defined in RFC4291.
	<i>prefix-length</i>	The length of the general prefix.
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	<p>It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.</p> <p>A general prefix could contain multiple prefixes.</p>	

These longer specified prefixes are usually used for the IPv6 address configuration on the interface.

Configuration The following example configures manually a general prefix as my-prefix.

Examples Ruijie(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48

Related Commands	Command	Description
	ipv6 address prefix-name sub-bits/prefix-length	Configures the interface address using the general prefix.
	show ipv6 general-prefix	Displays the general prefix.

Platform N/A

Description

3.7 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

ipv6 hop-limit *value*

no ipv6 hop-limit

Parameter	Parameter	Description
Description	<i>value</i>	The number of hop ranging from 1 to 255.

Defaults The default is 64.

Command Mode Global configuration mode.

Usage Guide This command takes effect for the unicast messages only, not for multicast messages.

Configuration Examples Ruijie(config)# ipv6 hop-limit 100

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.8 ipv6 icmp error-interval

Use this command to set the frequency with which ICMPv6-oversize error packets are sent. Use the no form of this command to restore the default setting.

ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]
no ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]

Use this command to set the frequency with which other ICMPv6 error packets are sent. Use the no form of this command to restore the default setting.

ipv6 icmp error-interval *milliseconds* [*bucket-size*]
no ipv6 icmp error-interval *milliseconds* [*bucket-size*]

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Sets the refresh interval of the token bucket, in the range from 0 to 2147483647 in the unit of seconds. Setting the value to 0 indicates that the frequency with which ICMPv6 error packets are sent is not fixed.
	<i>bucket-size</i>	Sets the number of tokens in the token bucket, in the range from 1 to 200.

Defaults The default milliseconds is 100 and bucket-size is 10.

Command Global configuration mode

Mode

Usage Guide The token bucket algorithm is adopted to set the frequency with which ICMPv6 error packets are sent so as to prevent Denial of Service (DoS) attack, If the forwarded IPv6 packet is greater than the egress IPv6 MTU in size, the router discards the IPv6 packet and sends the ICMPv6-oversize error packet to the source IPv6 address. This kind of ICMPv6 error packet is used for IPv6 path MTU discovery. If there are too many ICMPv6 error packets, the ICMPv6-oversize error packet may not be sent, causing IPv6 path MTU discovery failure. Therefore, it is recommended to set the frequency of ICMPv6-oversize error packet and other ICMPv6 error packet respectively. Note that ICMPv6 redirect packet is not an ICMPv6 error packet and Ruijie sets the frequency of the ICMPv6 redirect packet the same as that of other ICMPv6 error packet. For the timer is accurate to 10 milliseconds, it is recommended to set the refresh interval of the token bucket to an integer multiple of 10 milliseconds. If the refresh interval is not an integer multiple of 10 milliseconds, it is converted automatically. For example, the frequency of 1 per five milliseconds turns out to be 2 per 10 milliseconds; the frequency of 3 per 15 milliseconds is converted to 2 per 10 milliseconds.

Configuration Examples The following example sets the frequency with which ICMPv6-oversize error packets are sent to 100 per second.

```
Ruijie(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the frequency with which other ICMPv6 error packets are sent to 10 per second.

```
Ruijie(config)# ipv6 icmp error-interval 1000 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.9 ipv6 mtu

Use this command to configure the MTU of IPv6 packets. Use the no form of this command to restore the default setting.

ipv6 mtu *bytes*
no ipv6 mtu

Parameter	Parameter	Description
Description	<i>bytes</i>	MTU of IPv6 packets, in bytes. The value ranges from 1280 to 1500.

Defaults The default configuration is the same as the configuration of the mtu command.

Command Mode Interface configuration mode

Usage Guide If the size of an IPv6 packet exceeds the IPv6 MTU, the RGOS software segments the packet. For all devices in the same physical network segment, the IPv6 MTU of the interconnected interface must be the same.

Configuration Examples The following example sets the IPv6 MTU of the FastEthernet 0/1 interface to 1400 bytes.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 mtu 1400
```

Related Commands	Command	Description
	mtu	Sets the MTU of an interface.

Platform Description This command cannot be used on Layer 2 devices.

3.10 ipv6 nd cache interface-limit

Use this command to set the maximum number of neighbors learned on the interface. Use the no form of this command to restore the default setting.

ipv6 nd cache interface-limit *value*
no ipv6 nd cache interface-limit

Parameter	Parameter	Description
Description	<i>value</i>	Sets the maximum number of neighbors learned on the interface, including the static and dynamic

	neighbors, in the range from 0 to the number supported by the device. 0 indicates the number is not limited.
--	--

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. limit must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.

Configuration Examples The following example sets the number of neighbors learned on the interface to 100.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.11 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the no form of this command to restore it to the default setting.

`ipv6 nd dad attempts value`

`no ipv6 nd dad attempts value`

Parameter Description	Parameter	Description
	<i>value</i>	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

Defaults The default is 1.

Command Mode Interface configuration mode.

Usage Guide When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the "tentative" status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that

the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

Configuration Examples `Ruijie(config-if)# ipv6 nd dad attempts 3`

Examples

Related Commands	Command	Description
	<code>show ipv6 interface</code>	Displays the interface information.

Platform N/A

Description

3.12 Ipv6 nd dad retry

Use this command to set the interval for address conflict detection. Use the no form of this command to restore the default setting.

ipv6 nd dad retry value

no ipv6 nd dad retry

Parameter Description	Parameter	Description
	<i>value</i>	Sets the interval for address conflict detection, 60 seconds by default. Setting value to 0 indicates that the function is disabled.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the conflict address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.

Configuration Examples **The following example sets the interval for address conflict detection to 10s.**

`Ruijie(config)# ipv6 nd dad retry 10`

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.13 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to restore the default setting.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command

Mode Interface configuration mode.

Usage Guide This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.

Configuration Ruijie(config-if)# ipv6 nd managed-config-flag

Examples

Related	Command	Description
Commands	show ipv6 interface	Displays the interface information.
	ipv6 nd other-config-flag	Sets the flag for obtaining all information except IP address through stateful auto configuration.

Platform N/A

Description

3.14 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore the default setting.

ipv6 nd ns-interval milliseconds

no ipv6 nd ns-interval

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds

Defaults The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000 milliseconds (1 second).

Command mode Interface configuration mode.

Usage Guide The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

Configuration Examples

```
Ruijie(config-if)# ipv6 nd ns-interval 2000
```

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.

Platform Description N/A

3.15 ipv6 nd other-config-flag

Use this command to set "other stateful configuration" flag bit of the RA message. Use the no form of this command to delete the flag bit.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The flag bit is not set by default.

Command mode Interface configuration mode.

Usage Guide With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

Configuration Examples

```
Ruijie(config-if)# ipv6 nd other-config-flag
```

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.

Platform N/A
Description

3.16 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the no form of this command to delete the set prefix or restore the default setting.

```
ipv6 nd prefix { ipv6-prefix/prefix-length | default } [ [ valid-lifetime preferred-lifetime ] ] [ at
valid-date preferred-date ] [ [ infinite | preferred-lifetime ] ] [ no-advertise ] [ [ off-link ]
[ no-autoconfig ] ] [ [ pool pool-name ] ]
no ipv6 nd prefix { ipv6-prefix/prefix-length | default }
```

Parameter	Parameter	Description
Description	<i>ipv6-prefix</i>	IPv6 network ID following the format defined in RFC4291
	<i>prefix-length</i>	Length of the IPv6 prefix. “/” shall be added in front of the prefix
	<i>valid-lifetime</i>	Valid lifetime of the RA prefix received by the host
	<i>preferred-lifetime</i>	Preferred lifetime of the RA prefix received by the host
	<i>at valid-date preferred-date</i>	Sets the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
	infinite	Indicates that the prefix is always valid.
	default	Sets the default prefix.
	no-advertise	The prefix will not be advertised by the device.
	off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
	no-autoconfig	Indicates that the RA prefix received by the host cannot be used for auto address configuration.
	pool pool-name	Indicates the IPv6 prefix pool

Defaults By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:

valid-lifetime: 2592000s (30 days)

preferred-lifetime: 604800s (7 days),

The prefix is advertised and is used for on-link judgment and auto address configuration.

Command Interface configuration mode.
Mode

Usage Guide This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

ipv6 nd prefix default

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

at valid-date preferred-date

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

Configuration The following example adds a prefix for SVI 1.

Examples

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 prefix default no-autoconfig
```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related Commands	Command	Description
	show ipv6 interface	Displays the RA information of an interface.

Platform N/A

Description

3.17 ipv6 nd ra-hoplimit

Use this command to set the hopcount of the RA message. Use the no form of this command to restore the default setting.

ipv6 nd ra-hoplimit value

no ipv6 nd ra-hoplimit

Parameter Description	Parameter	Description
	<i>value</i>	Hopcount

Defaults The default is 64.

Command Mode Interface configuration mode.

Usage Guide This command is used to set the hopcount of the RA message.

Configuration Ruijie(config-if)# ipv6 nd ra-hoplimit 110

Examples

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-lifetime	Sets the lifetime of the device.
	ipv6 nd ra-interval	Sets the interval of sending the RA message.
	ipv6 nd ra-mtu	Sets the MTU of the RA message.

Platform N/A

Description

3.18 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the no form of this command to restore the default setting.

ipv6 nd ra-interval { *seconds* | **min-max** *min_value* *max_value* }

no ipv6 nd ra-interval

Parameter	Parameter	Description
Description	<i>seconds</i>	Interval of sending the RA message in seconds, 3-1800s.
	min-max	Maximum and minimum interval sending the RA message in seconds
	<i>min_value</i>	Minimum interval sending the RA message in seconds
	<i>max_value</i>	Maximum interval sending the RA message in seconds

Defaults 200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.

Command Interface configuration mode.

Mode

Usage Guide If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

Configuration Ruijie(config-if)# ipv6 nd ra-interval 110

Examples Ruijie(config-if)# ipv6 nd ra-interval min-max 110 120

Related	Command	Description
---------	---------	-------------

Commands	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-lifetime	Sets the lifetime of the device.
	ipv6 nd ra-hoplimit	Sets the hopcount of the RA message.
	ipv6 nd ra-mtu	Sets the MTU of the RA message.

Platform N/A

Description

3.19 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the no form of this command to restore the default setting.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameter	Parameter	Description
Description	<i>seconds</i>	Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds.

Defaults The default is 1800.

Command Interface configuration mode.

Mode

Usage Guide The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

Configuration Ruijie(config-if)# ipv6 nd ra-lifetime 2000

Examples

Related	Command	Description
Commands	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-interval	Sets the interval of sending the RA.
	ipv6 nd ra-hoplimit	Sets the hopcount of the RA.
	ipv6 nd ra-mtu	Sets the MTU of the RA.

Platform N/A

Description

3.20 ipv6 nd ra-mtu

Use this command to set the MTU of the RA message. Use the no form of this command to restore the default setting.

ipv6 nd ra-mtu *value*

no ipv6 nd ra-mtu

Parameter	Parameter	Description
Description	<i>value</i>	MTU value, in the range from 0 to 4294967295.

Defaults IPv6 MTU value of the network interface.

Command Mode Interface configuration mode.

Mode

Usage Guide If it is specified as 0, the RA will not have the MTU option

Configuration Examples

```
Ruijie(config -if)# ipv6 nd ra-mtu 1400
```

Examples

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-lifetime	Sets the lifetime of the device.
	ipv6 nd ra-interval	Sets the interval of sending the RA message.
	ipv6 nd ra-hoplimit	Sets the hopcount of the RA message.

Platform N/A

Description

3.21 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the no form of this command to restore the default setting.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Reachable time for the neighbor in the range from 0 to 3600000 in the unit of milliseconds.

Defaults The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000 milliseconds (30 seconds) when the device discovers the neighbor.

Command Interface configuration mode.

Mode

Usage Guide The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time.

The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.

Configuration Examples

```
Ruijie(config-if)# ipv6 nd reachable-time 1000000
```

Examples

Related Commands	Command	Description
	<code>show ipv6 interface</code>	Displays the interface information.

Platform N/A

Description

3.22 ipv6 nd state-time

Use this command to set the period for the neighbor to maintain the state. Use the no form of this command to restore the default setting.

ipv6 nd state-time *seconds*

no ipv6 nd state-time

Parameter	Parameter	Description
Description	<i>Seconds</i>	Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.

Defaults The default is 3600.

Command Global configuration mode

Mode

Usage Guide This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.

Configuration Examples The following example sets the period to 600 seconds for the neighbor to maintain the state.

```
Ruijie(config)# ipv6 nd stale-time 600
```

Related	Command	Description
---------	---------	-------------

Commands	N/A	N/A
-----------------	-----	-----

Platform N/A

Description

3.23 ipv6 nd suppress-auth-vlan-ns

Use this command to disable the SVI interface from sending the NS packet to the authentication VLAN. Use the no form of this command to disable this function.

ipv6 nd suppress-auth-vlan-ns

no ipv6 nd suppress-auth-vlan-ns

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide This command is supported on the SVI interface in gateway authentication mode.

Configuration Examples The following example enables VLAN 2 to send the NS packet to the authentication VLAN.

```
Ruijie(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

3.24 ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message. Use the no form of this command to enable the function.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The **ipv6 nd suppress-ra** command is enabled by default.

Command Interface configuration mode.

Mode

Usage Guide This command suppresses the sending of the RA message on an interface.

Configuration Examples `Ruijie(config-if)# ipv6 nd suppress-ra`

Related Commands	Command	Description
	<code>show ipv6 interface</code>	Displays the interface information.

Platform N/A

Description

3.25 ipv6 nd threshold

Use this command to configure the neighbor entry threshold to prevent ND-based Dos attacks. Use the no form of this command to restore the default setting.

`ipv6 nd threshold percent_value`

`no ipv6 nd threshold`

Parameter	Parameter	Description
Description	<i>percent_value</i>	Neighbor entry threshold, in the range from 50 to 100.

Defaults The default is 70.

Command Mode Global configuration mode.

Usage Guide The threshold indicates the percentage of current neighbor entry count accounting for the maximum count. When the IPv6 neighbor entry count reaches the threshold, reachability test will be performed on neighbors in the stale state. But it does not affect the neighbor discovery function. The device can still learn new neighbor entries.

Configuration Examples The following example sets the threshold to 80%.

`Ruijie(config)# ipv6 nd threshold 80`

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.26 ipv6 nd threshold per-mac

Use this command to configure the maximum neighbor entry count for a MAC address to prevent ND-based Dos attacks. Use the no form of this command to restore the default setting.

ipv6 nd threshold per-mac *value*

no ipv6 nd threshold per-mac

Parameter	Parameter	Description
Description	<i>value</i>	Neighbor entry count, in the range from 4 to 256.

Defaults The default is 16.

Command Mode Global configuration mode.

Usage Guide When the IPv6 neighbor entry count reaches the threshold, reachability test will be performed on neighbors in the stale state. But it does not affect the neighbor discovery function. The device can still learn new neighbor entries.

Configuration The following example sets the count to 100.

Examples Ruijie(config)# ipv6 nd threshold per-mac 100

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

3.27 ipv6 nd unresolved

Use this command to set the maximum number of the unresolved neighbor table entries. Use the no form of this command to restore the default setting.

ipv6 nd unresolved *number*

no ipv6 nd unresolved

Parameter	Parameter	Description
Description	<i>number</i>	Sets the maximum number of the unresolved neighbor table entries, in the range from 1 to the neighbor table size supported by the device.

Defaults The default is 0. (The maximum number is the neighbor table size supported by the device)

Command Global configuration mode

Mode

Usage Guide This command is used to prevent unresolved ND table entries generated by malicious scan attacks from consuming table entry resources,

Configuration The following example sets the maximum number of the unresolved neighbor table entries to 200.

Examples Ruijie(config)# ipv6 nd unresolved 200

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

3.28 ipv6 neighbor

Use this command to configure a static neighbor. Use the no form of this command to delete a static neighbor.

ipv6 neighbor *ipv6-address interface-id hardware-address*

no ipv6 neighbor *ipv6-address interface-id*

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	The neighbor IPv6 address, in the form as defined in RFC4291.
	<i>interface-id</i>	Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface).
	<i>hardware-address</i>	The 48-bit MAC address, a dotted triple of four-digit hexadecimal numbers.

Defaults No static neighbor is configured by default.

Command Global configuration mode

Mode

Usage Guide This command can only be configured on the interface enabled with IPv6 protocol, similar to the ARP command.

If the neighbor to be configured has been learned through Neighbor Discovery Protocol (NDP) and stored in the NDP neighbor table, the dynamic neighbor turns to be static. If the static neighbor is valid, it is always reachable. An invalid static neighbor refers to the neighbor whose IPv6 address is not valid (not in the IPv6 network segment configured for the interface or interface address conflict). The packet is not forwarded to the MAC address as specified by the invalid static neighbor. The invalid static neighbor is in inactive state. Use the show ipv6 neighbor static command to display the state of the static neighbor.

Use the `clear ipv6 neighbors` command to clear all neighbors learned dynamically through NDP.

Configuration The following example configures a static neighbor on SVI 1.

Examples

```
Ruijie(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.29 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. Use the `no` form of this command to use the global IP address `w` as the source address to send neighbor requests.

ipv6 ns-linklocal-src
no ipv6 ns-linklocal-src

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The local address of the link is always used as the source address to send neighbor requests.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# no ipv6 ns-linklocal-src
```

Examples

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.30 ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the `no` form of this command to restore the default setting.

ipv6 redirects
no ipv6 redirects

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Interface configuration mode.

Mode

Usage Guide The transmission rate of any ICMPv6 error message is limited. By default, it is 10pps.

Configuration The following example enables ICMPv6 redirection on interface GigabitEthernet 0/1.

Examples

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 redirects
```

Related	Command	Description
Commands	show ipv6 interface	Displays the interface information.

Platform N/A

Description

3.31 ipv6 source-route

Use this command to forward the IPv6 packet with route header. Use the no form of this command to restore the default setting.

ipv6 source-route
no ipv6 source-route

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The **ipv6 source-route** command is disabled by default.

Command Global configuration mode.

Mode

Usage Guide Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.

Configuration

```
Ruijie(config)# no ipv6 source-route
```

Examples

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.32 show ipv6 address

Use this command to display the IPv6 addresses.

show ipv6 address [*interface-name*]

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Mode

Usage Guide N/A

Configuration The following example displays all IPv6 address configured on the device.

Examples

```
Ruijie#show ipv6 address
Global unicast address limit: 1024, Global unicast address count: 3
Tentative address count: 2,Duplicate address count: 1
Preferred address count: 3,Deprecated address count: 0
Gi 0/5
  FE80::1/64 Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  1000::1/64 Duplicate
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Gi 0/6
  FE80::1/64 Tentative
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  1111:1111:1111:1111:1111:1111:1111:1111/64 Tentative
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Gi 0/7
  FE80::1/64 Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  2000:1111:1111:1111:1111:1111:1111:1111/64 Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

The following example displays the IPv6 address configured on the GigabitEthernet 0/1.

```
Ruijie#show ipv6 address Gi 0/5
Global unicast address count: 3
Tentative address count: 0,Duplicate address count: 1
Preferred address count: 1,Deprecated address count: 0
FE80::1/64 Preferred
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
1000::1/64 Duplicate
Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

3.33 show ipv6 general-prefix

Use this command to display the information of the general prefix.

show ipv6 general-prefix

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

Configuration Examples

```
The following example displays the information of the general prefix.
Ruijie#
show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix my-prefix, acquired via Manual configuration
2001:1111:2222::/48
2001:1111:3333::/48
```

Related	Command	Description
Commands	ipv6 general-prefix	Configures the general prefix.

Platform N/A
Description

3.34 show ipv6 interface

Use this command to display the IPv6 interface information.

show ipv6 interface [*interface-id*] [**ra-info**] [**brief** [*interface-id*]]

Parameter	Parameter	Description
Description	<i>interface-id</i>	Interface (including Ethernet interface, aggregate port, or SVI)
	ra-info	Displays the RA information of the interface.
	<i>brief</i>	Displays the brief information of the interface (interface status and address information).

Defaults N/A

Command Mode N/A

Usage Guide Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.

Configuration The following example displays the information of the IPv6 interface.

Examples

```
Ruijie# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
```

```
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds
```

The following line is included in the above information: 2001::1, subnet is 2001::/64 [TENTATIVE].
The flag bit in the [] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.

```
The following example displays the RA information of the IPv6 interface.Ruijie#
show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags: LA)
```

Description of the fields in ra-info:

Field	Meaning
RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.
initcount	Indicate the number of the RAs when the RA timer is restarted.

RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	Meaning
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicate that the interfaces use the default prefix.
Auto CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.
vlttime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.
L !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

The following example displays the brief information of the IPv6 interface.

```
Ruijie#show ipv6 interface brief
GigabitEthernet 0/1          [down/down]
    2222::2
    FE80::1614:4BFF:FE5C:ED3A
```

Related Commands	Command	Description
	N/A	N/A

Platform Description
N/A

3.35 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

show ipv6 neighbors [vrf *vrf-name*] [**verbose**] [*interface-id*] [*ipv6-address*] [**static**] [**oob**]

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name
	verbose	Displays the neighbor details.
	<i>interface-id</i>	Displays the neighbors of the specified interface.
	<i>ipv6-address</i>	Displays the neighbors of the specified IPv6 address.
	static	Displays the validity status of static neighbors.
	oob	Displays the dynamic IPv6 neighbors discovered by neighbors on MGMT interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the neighbors on the SVI 1 interface: Ruijie# show

```

ipv6 neighbors vlan 1
IPv6 Address Linklayer Addr Interface
fa::1 00d0.0000.0002 vlan 1
fe80::200:ff:fe00:2 00d0.0000.0002 vlan 1
Show the neighbor details:
Ruijie# show ipv6 neighbors verbose
IPv6 Address Linklayer Addr Interface
2001::1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0

```

Field	Meaning
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.
Interface	Interface the neighbor locates.
State	State of the neighbor: state/H(R) The values of STATE are as below:

	<p>INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received.</p> <p>REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor.</p> <p>STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor.</p> <p>DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD.</p> <p>PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3).</p> <p>?: Unknown state.</p> <p>/R—indicate the neighbor is considered as a device</p> <p>/H: The neighbor is a host.</p>
Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

Related Commands	Command	Description
	ipv6 neighbor	Configures a neighbor.

Platform N/A
Description

3.36 show ipv6 neighbors statistics

Use the following commands to display the statistics of one IPv6 neighbor.

show ipv6 neighbors [vrf vrf-name] statistics [all]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	all	Displays the statistics of all IPv6 neighbors.

Defaults N/A

Command Privileged EXEC mode.

Mode

Usage Guide N/A

Configuration The following example displays the statistics of the global neighbors.

Examples

```
Ruijie#show ipv6 neighbor statistics

Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0
Ruijie#
```

The following example displays the statistics of all IPv6 neighbors.

```
Ruijie#show ipv6 neighbor statistics all

IPv6 neighbor table count: 1
Static neighbor count: 0(0 active, 0 inactive)
Total
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;

Global
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
Ruijie#
```

Related	Command	Description
Commands	N/A	N/A

Platform Supported on all platforms.

Description

3.37 show ipv6 packet statistics

Use this command to display the statistics of IPv6 packets.

show ipv6 packet statistics [total | *interface-name*]

Parameter	Parameter	Description
-----------	-----------	-------------

Description	total	Displays total statistics of all interfaces.
	<i>interface-name</i>	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the total statistics of the IPv6 packets and the statistics of each interface.

```
Ruijie#show ipv6 pack statistics
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
GigabitEthernet 0/5
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
Ruijie#
```

The following example displays the total statistics of the IPv6 packets.

```
Ruijie#show ipv6 pack statistics total
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
  Discards:0
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
Ruijie#
```

Related	Command	Description
Commands	N/A	N/A

Platform Supported on all platforms.

Description

3.38 show ipv6 packet statistics per-mac

Use this command to display the number of neighbor entries of every MAC address.

show ipv6 neighbor statistics per-mac [interface-name] [mac-address]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface ID
	<i>mac-address</i>	MAC address

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the number of neighbor entries of every MAC address..

Examples

```
Ruijie# show ipv6 neighbor statistics per-mac
Interface  MAC address      Statistics
-----
VLAN 1    0000:0000:0001    3
VLAN 1    0000:0000:0002    5
VLAN 2    0000:0000:0003    10
```

Field	Description
Interface	Interface ID.
MAC address	MAC address.
Statistics	ND entry number.

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

3.39 show ipv6 raw-socket

Use this command to display all IPv6 raw sockets.

show ipv6 raw-socket [num]

Parameter	Parameter	Description
Description	<i>num</i>	Protocol.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays all IPv6 raw sockets.

Examples

```
Ruijie# show ipv6 raw-socket
Number Protocol Process name
1      ICMPv6   vrrp.elf
2      ICMPv6   tcpip.elf
3      VRRP    vrrp.elf
Total: 3
```

Field	Description
Number	Number.
Protocol	Protocol.
Process name	Process number.
Total	Total number of IPv6 raw sockets.

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

3.40 show ipv6 routers

In the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to display the neighbor routers and the advertisement.

show ipv6 routers [*interface-type interface-number*]

Parameter	Parameter	Description
-----------	-----------	-------------

Description	<i>interface-type</i> <i>interface-number</i>	(Optional) Displays the routing advertisement of the specified interface.
--------------------	--	---

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.

Configuration The following example displays the IPv6 router

Examples

```
Ruijie# show ipv6 routers
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
Preference=MEDIUM
Reachable time 0 msec, Retransmit time 0 msec
Prefix 6001:3::/64 onlink autoconfig
Valid lifetime 2592000 sec, preferred lifetime 604800 sec
Prefix 6001:2::/64 onlink autoconfig
```

Valid lifetime 2592000 seconds, preferred lifetime 604800 seconds

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.41 show ipv6 sockets

Use this command to display all IPv6 sockets.

show ipv6 sockets

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays all IPv6 sockets.

Examples

```
Ruijie# show ipv6 sockets
Number Process name      Type  Protocol  LocalIP:Port  ForeignIP:Port  State
1      vrrp.elf             RAW   ICMPv6    :::58         :::0            *
2      tcpip.elf           RAW   ICMPv6    :::58         :::0            *
3      vrrp.elf             RAW   VRRP      :::112        :::0            *
4      rg-snmpd            DGRAM  UDP       :::161        :::0            *
5      rg-snmpd            DGRAM  UDP       :::162        :::0            *
6      dhcp6.elf           DGRAM  UDP       :::547        :::0            *
7      rg-sshd             STREAM TCP       :::22         :::0            LISTEN
8      rg-telnetd          STREAM TCP       :::23         :::0            LISTEN
Total: 8
```

Field	Description
Number	Number.
Process name	Process name.
Type	Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.
Protocol	Protocol number
LocalIP:Port	Local IPv6 address and port.
ForeignIP:Port	Peer IPv6 address and port.
State	State (for IPv6 TCP sockets).
Total	Total number of sockets.

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

3.42 show ipv6 udp

Use this command to display all IPv6 UDP sockets.

show ipv6 udp [local-port num] [peer-port num]

Use this command to display IPv6 UDP socket statistics.

show ipv6 udp statistics

**Parameter
Description**

Parameter	Description
local-port num	Local port number.
peer-port num	Peer port number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays all IPv6 UDP sockets.

Examples

```
Ruijie# show ipv6 udp
Number Local Address Peer Address Process name
1 :::161 :::0 rg-snmpd
2 :::162 :::0 rg-snmpd
3 :::547 :::0 dhcp6.elf
```

Filed	Description
Number	Number.
Local Address	Local IPv6 address and port.
Peer Address	Peer IPv6 address and port.
Process name	Process name.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4 DHCP Commands

4.1 address range

Use this command to specify the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool. Use the **no** form of this command to restore the default setting.

address range *low-ip-address high-ip-address*

no address range

Parameter	Parameter	Description
Description	<i>low-ip-address</i>	Start address in the network segment range.
	<i>high-ip-address</i>	End address in the network segment range.

Defaults By default, the associated CLASS is not configured with the network segment range. The default is the address pool range.

Command Mode Address pool CLASS configuration mode.

Usage Guide Each CLASS corresponds to one network range which must be from low address to high address, so as to allow the duplication of network segment range between multiple CLASSes. If the CLASS associated with the address pool is specified without configuring the corresponding network segment range, the default network segment range of this CLASS is same as the range of the address pool where this CLASS is.

Configuration Examples The following example configures the network segment of class1 associated with address pool mypool0 ranging from 172.16.1.1 to 172.16.1.8.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
Ruijie (config-dhcp-pool-class)# address range 172.16.1.1 172.16.1.8
```

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	class	Configures the CLASS associated with the DHCP address pool and enters the address pool CLASS configuration mode.

Platform Description N/A

4.2 address-manage

Use this command to enter the AM rule configuration mode.

address-manage

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is configured on the DHCP server and used in combination with Super VLAN.

Configuration Examples The following example enters the AM rule configuration mode.

```
Ruijie(config)#address-manage
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.3 bootfile

Use this command to define the startup mapping file name of the DHCP client. Use the **no** or **default** form of this command to restore the default setting.

bootfile file-name

no bootfile

default bootfile

Parameter	Parameter	Description
Description	<i>file-name</i>	Startup file name.

Defaults No startup file name is defined by default.

Command Mode DHCP address pool configuration mode

Usage Guide Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients

can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

Configuration The following example defines the device.conf as the startup file name.

Examples `bootfile device.conf`

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	next-server	Configures the next server IP address of the DHCP client startup process.

Platform N/A

Description

4.4 class

Use this command to configure the associated CLASS in the DHCP address pool. Use the **no** form of this command to restore the default setting.

class *class-name*
no class *class-name*

Parameter Description	Parameter	Description
	<i>class-name</i>	Class name, which can be the character string or numeric such as myclass or 1.

Defaults By default, no CLASS is associated with the address pool.

Command Mode DHCP address pool configuration mode

Usage Guide Each DHCP address pool performs the address assignment according to the Option82 matching information. We can divide this Option82 information into classes and specify the available network segment range for these classes in the DHCP address pool. These classes are called CLASS. One DHCP address pool can map to multiple CLASSES, and each CLASS can specify different network segment range.

During the address assignment, firstly, ensure the assignable address pool through the network segment where the client is, then according to the Option82 information further ensure the CLASS and assign the IP address from the network segment range corresponding to the CLASS. If one request packet matches multiple CLASSES in the address pool, perform the address assignment according to the sequencing of configuring the CLASS in the address pool. If this CLASS's assigned addresses have been to the upper limit, then continue to assign the address from the next CLASS, and so on. Each CLASS corresponds to one network segment range that must be from low addresses to high addresses and the duplicated network ranges between multiple CLASSES are allowed. If the CLASS corresponding to the address pool is specified and the network segment corresponding to the CLASS is not configured, this CLASS's default network segment range is same

as the range of address pool where the CLASS is.

Configuration The following example configures the address *mypool0* to associate with class1.

Examples

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
```

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.5 clear ip dhcp binding

Use this command to clear the DHCP binding table in the privileged user mode.

clear ip dhcp binding { * | *ip-address* }

Parameter	Parameter	Description
Description	*	Deletes all DHCP bindings.
	<i>ip-address</i>	Deletes the binding of the specified IP addresses.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the **no ip dhcp pool** command.

Configuration The following example clears the DHCP binding with the IP address 192.168.12.100.

Examples

```
clear ip dhcp binding 192.168.12.100
```

Related Commands	Command	Description
	show ip dhcp binding	Displays the address binding of the DHCP server.

Platform N/A

Description

4.6 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record.

clear ip dhcp conflict { * | *ip-address* }

Parameter	Parameter	Description
Description	*	Deletes all DHCP address conflict records.
	<i>ip-address</i>	Deletes the conflict record of the specified IP addresses.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The clear ip dhcp conflict command can be used to delete the history conflict record.	
Configuration Examples	The following example clears all address conflict records.	
Examples	<pre>clear ip dhcp conflict *</pre>	
Related Commands	Command	Description
	ip dhcp ping packets	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
	show ip dhcp conflict	Displays the address conflict that the DHCP server detects when it assigns an IP address.
Platform Description	N/A	

4.7 clear ip dhcp history

Use this command to clear the address assigned by the DHCP server.

clear ip dhcp history{ * | *mac-address* }

Parameter	Parameter	Description
Description	*	Clears all addresses assigned by the DHCP server.
	<i>mac-address</i>	Clears the address assigned by the DHCP server corresponding to the specified MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is configured on the DHCP server.	

Configuration The following example clears all addresses assigned by the DHCP server.

Examples

```
Ruijie# clear ip dhcp history *
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.8 clear ip dhcp relay statistics

Use this command to clear the DHCP relay statistics.

clear ip dhcp relay statistics

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The DHCP relay is configured with the counter to count various packets received or transmitted by the relay. This command is used to clear the counters.

Configuration The following example clears the DHCP relay statistics.

Examples

```
Ruijie# clear ip dhcp relay statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.9 clear ip dhcp server detect

Use this command to clear statistics about the fake DHCP server.

clear ip dhcp server detect { * | ip-address }

Parameter	Parameter	Description
Description	*	Clears statistics about all fake DHCP servers.
	<i>ip-address</i>	Clears statistics about the specified fake DHCP server.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The detected fake DHCP server addresses are saved on the server. You can use the **clear ip dhcp server detect** command to clear statistics about the fake DHCP server.

Configuration Examples The following example clears statistics about all fake DHCP servers.

```
Ruijie# clear ip dhcp server detect *
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.10 clear ip dhcp server rate

Use this command to clear statistics about the packet processing rate of every module.

clear ip dhcp server rate

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear statistics about the packet processing rate of every module, including arp, hot backup, lsm, and socket.

Configuration Examples The following example clears statistics about the packet processing rate of every module.

```
Ruijie# clear ip dhcp server rate
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.11 clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in the privileged user mode.

clear ip dhcp server statistics

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The **clear ip dhcp server statistics** command can be used to delete the history counter record and carry out the statistics starting from scratch.

Configuration Examples The following example clears the statistics record of the DHCP server.

```
clear ip dhcp server statistics
```

Related Commands	Command	Description
	show ip dhcp server statistics	Displays the statistics record of the DHCP server.

Platform Description N/A

4.12 client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

client-identifier *unique-identifier*

no client-identifier

default client-identifier

Parameter	Parameter	Description
Description	<i>unique-identifier</i>	The DHCP client ID is indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

Defaults N/A.

Command DHCP address pool configuration mode.

Mode

Usage Guide When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather than their hardware addresses. The client ID consists of media type, MAC addresses and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media. The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/1. For the definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700. This command is used only when the DHCP is defined by manual binding.

Configuration Examples The following example defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```
client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

Related Commands

Command	Description
hardware-address	Defines the hardware address of DHCP client.
host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.13 client-name

Use this command to define the name of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

- client-name** *client-name*
- no client-name**
- default client-name**

Parameter Description

Parameter	Description
client-name	Name of DHCP client, a set of standards-based ASCII characters. The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn.

Defaults No client name is defined by default.

Command DHCP address pool configuration mode.

Mode

Usage Guide This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.

Configuration The following example defines a string river as the name of the client.

Examples

```
client-name river
```

**Related
Commands**

Command	Description
host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.14 default-router

Use this command to define the default gateway of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

default-router *ip-address* [*ip-address2*...*ip-address8*]

no default-router

default default-router

**Parameter
Description**

Parameter	Description
<i>ip-address</i>	Defines the IP address of the equipment. It is required to configure one IP address at least.
<i>ip-address2</i> ... <i>ip-address8</i>	(Optional) Up to 8 gateways can be configured.

Defaults No gateway is defined by default.

Command DHCP address pool configuration mode.

Mode

Usage Guide In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.

Configuration The following example defines 192.168.12.1 as the default gateway.

Examples

```
default-router 192.168.12.1
```

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A
Description

4.15 dns-server

Use this command to define the DNS server of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

dns-server { *ip-address* [*ip-address2*...*ip-address8*] | **use-dhcp-client** *interface-type interface-number* }
no dns-server
default dns-server

Parameter Description	Parameter	Description
	<i>ip-address</i>	Defines the IP address of the DNS server. At least one IP address should be configured.
	<i>ip-address2</i> ... <i>ip-address8</i>	(Optional) Up to 8 DNS servers can be configured.
	use-dhcp-client <i>interface-type interface-number</i>	Uses the DNS server learned by the DHCP client of the RGOS software as the DNS server of the DHCP client.

Defaults No DNS server is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide When more than one DNS server is defined, the former will possess higher priority, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails. If the RGOS software also acts as the DHCP client, the DNS server information obtained by the client can be transmitted to the DHCP client.

Configuration Examples The following example specifies the DNS server 192.168.12.3 for the DHCP client.

```
dns-server 192.168.12.3
```

Related Commands	Command	Description
	domain-name	Defines the suffix domain name of the DHCP client.
	ip address dhcp	Enables the DHCP client on the interface to obtain the IP address information.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.16 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

domain-name *domain-name*

no domain-name

default domain-name

Parameter	Parameter	Description
Description	<i>domain-name</i>	Defines the suffix domain name string of the DHCP client.

Defaults No suffix domain name by default.

Command DHCP address pool configuration mode.

Mode

Usage Guide After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.

Configuration The following example defines the suffix domain name i-net.com.cn for the DHCP client.

Examples

```
Ruijie (dhcp-config) #domain-name ruijie.com.cn
```

Related	Command	Description
Commands	dns-server	Defines the DNS server of the DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.

Platform N/A

Description

4.17 force-no-router

Use this command to cancel gateway allocation to the client. Use the **no** or **default** form of this command to restore the default setting.

force-no-router

no force-no-router

default force-no-router

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode DHCP address pool configuration mode

Usage Guide N/A

Configuration The following example cancels gateway allocation to the client.

Examples Ruijie (dhcp-config) # force-no-router

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.18 hardware-address

Use this command to define the hardware address of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

hardware-address *hardware-address* [*type*]

no hardware-address

default hardware-address

Parameter Description	Parameter	Description
	<i>hardware-address</i>	Define the MAC address of the DHCP client.
	<i>type</i>	To indicate the hardware platform protocol of the DHCP client, use the string definition or digits definition. String option: Ethernet ieee802 Digits option: 1 (10M Ethernet) 6 (IEEE 802)

Defaults No hardware address is defined by default.
If there is no option when the hardware address is defined, it is the Ethernet by default.

Command Mode DHCP address pool configuration mode.

Usage Guide This command can be used only when the DHCP is defined by manual binding.

Configuration The following example defines the MAC address 00d0.f838.bf3d with the type ethernet.

Examples `hardware-address 00d0.f838.bf3d`

Related Commands	Command	Description
	client-identifier	Defines the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot).
	host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	default-router	Defines the default route of the DHCP client.

Platform N/A

Description

4.19 host

Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

host *ip-address* [*netmask*]

no host

default host

Parameter Description	Parameter	Description
	host <i>ip-address</i>	Defines the IP address of DHCP client.
	<i>netmask</i>	Defines the network mask of DHCP client.

Defaults No IP address or network mask of the host is defined.

Command Mode DHCP address pool configuration mode.

Usage Guide If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address.

This command can be used only when the DHCP is defined by manual binding.

Configuration Examples The following example sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240.

```
host 192.168.12.91 255.255.255.240
```

Related Commands	Command	Description
	client-identifier	Defines the unique ID of the DHCP client (Indicated in hex and

	separated by dot).
hardware-address	Defines the hardware address of DHCP client.
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
default-router	Define the default route of the DHCP client. default-router

Platform N/A

Description

4.20 ip address dhcp

Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

ip address dhcp

no ip address dhcp

default ip address dhcp

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The interface cannot obtain the IP address by the DHCP by default.

Command Interface configuration mode.

Mode

Usage Guide When requesting the IP address, the DHCP client of the RGOS software also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information (optional).

The client of the RGOS software is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server. At present, our server can support this function.

Configuration The following example makes the FastEthernet 0 port obtain the IP address automatically.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1) ip address dhcp
```

Related Commands	Command	Description
	dns-server	Defines the DNS server of DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A
Description

4.21 ip dhcp class

Use this command to define a CLASS and enter the global CLASS configuration mode. Use the **no** form of this command to restore the default setting.

ip dhcp class *class-name*

no ip dhcp class *class-name*

Parameter	Parameter	Description
Description	<i>class-name</i>	Class name, which can be character string or numeric such as myclass or 1.

Defaults By default, the class is not configured.

Command Mode Global configuration mode.

Usage Guide After executing this command, it enters the global CLASS configuration mode which is shown as "Ruijie (config-dhcp-class)#". In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.

Configuration The following example configures a global CLASS.

Examples Ruijie(config)# ip dhcp class myclass

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.22 ip dhcp excluded-address

Use this command to define some IP addresses and make the DHCP server not assign them to the DHCP client in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

no ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

default ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

Parameter	Parameter	Description
Description	<i>low-ip-address</i>	Excludes the IP address, or excludes the start IP address within the range

	of the IP address.
<i>high-ip-address</i>	Excludes the end IP address within the range of the IP address.

Defaults The DHCP server assigns the IP addresses of the whole address pool by default.

Command Mode Global configuration mode.

Usage Guide If the excluded IP address is not configured, the DHCP server attempts to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts to prevent these addresses are assigned to the DHCP client, and define the excluded IP address accurately to reduce the conflict detecting time when the DHCP server assigns the address.

Configuration Examples In the following example, the DHCP server will not attempt to assign the IP addresses within 192.168.12.100~150.

```
ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	network (DHCP)	Defines the network number and network mask of the DHCP address pool.

Platform Description N/A

4.23 ip dhcp force-send-nak

Use this command to configure the forcible NAK packet sending function. Use the **no** or **default** form of this command to restore the default setting.

ip dhcp force-send-nak
no ip dhcp force-send-nak
default ip dhcp force-send-nak

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide The DHCP client checks the previously used IP address every time it is started and sends a DHCPREQUEST packet to continue leasing this IP address. If the address is not available, the DHCP server sends an NAK packet to let the client resend a DHCPDISCOVER packet to apply for a new IP address. If no corresponding lease record can be found on the server, the client keeps sending DHCPDISCOVER packets.

Configuration Examples The following example enables the forcible NAK packet sending function in global configuration mode.

```
Ruijie(config)# ip dhcp force-send-nak
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.24 ip dhcp monitor-vrrp-state

Use this command in layer-3 configuration mode to enable the DHCP Server to monitor the status of VRRP interfaces so that the DHCP Server processes only those packets sent from a VRRP interface in the Master state. Use the **no** or **default** form of this command to restore the default setting. If it is canceled, the DHCP Server processes packets from VRRP interfaces in the Master or Backup state.

- ip dhcp monitor-vrrp-state**
- no ip dhcp monitor-vrrp-state**
- default ip dhcp monitor-vrrp-state**

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The **ip dhcp monitor-vrrp-state** command is disabled by default. .

Command Mode Layer-3 interface configuration mode.

Usage Guide If a VRRP address is configured for an interface, the DHCP Server processes packets sent from the master interface and discards packets sent from the backup interface. If no VRRP address is configured, the DHCP Server does not monitor the status of VRRP interfaces. All DHCP packets will be processed.

Configuration Examples The following example enables the DHCP Server to monitor the status of VRRP interfaces.

```
Ruijie(config-if)# ip dhcp monitor-vrrp-state
```

Related	Command	Description
---------	---------	-------------

Commands	N/A	N/A
-----------------	-----	-----

Platform N/A

Description

4.25 ip dhcp ping packets

Use this command to configure the times of pinging the IP address when the DHCP server detects address conflict in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

ip dhcp ping packets [*number*]

no ip dhcp ping packets

default ip dhcp ping packets

Parameter	Parameter	Description
Description	<i>number</i>	(Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default.

Defaults The Ping operation sends two packets by default.

Command Mode Global configuration mode.

Usage Guide When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.

Configuration Examples The following example sets the number of the packets sent by the ping operation as 3.

```
ip dhcp ping packets 3
```

Related Commands	Command	Description
	clear ip dhcp conflict	Clears the DHCP history conflict record.
	ip dhcp ping packet	Configures the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned. Otherwise, it will record the address conflict.
	show ip dhcp conflict	Displays the DHCP server detects address conflict when it assigns an IP address.

Platform N/A

Description

4.26 ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

ip dhcp ping timeout *milli-seconds*

no ip dhcp ping timeout

default ip dhcp ping timeout

Parameter	Parameter	Description
Description	<i>milli-seconds</i>	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

Defaults The default is 500 seconds.

Command Global configuration mode.

Mode

Usage Guide This command defines the time that the DHCP server waits for a ping response packet.

Configuration The following example configures the waiting time of the ping response packet to 600ms.

Examples

```
ip dhcp ping timeout 600
```

Related	Command	Description
Commands	clear ip dhcp conflict	Clears the DHCP history conflict record.
	ip dhcp ping packets	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
	show ip dhcp conflict	Displays the address conflict the DHCP server detects when it assigns an IP address.

Platform N/A

Description

4.27 ip dhcp pool

Use this command to define a name of the DHCP address pool and enter the DHCP address pool configuration mode in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

ip dhcp pool *pool-name*

no ip dhcp pool *pool-name*

default ip dhcp pool *pool-name*

Parameter	Parameter	Description
Description	<i>pool-name</i>	A string of characters and positive integers, for instance, mypool or 1.

Defaults No DHCP address pool is defined by default.

Command Mode Global configuration mode.

Usage Guide Execute the command to enter the DHCP address pool configuration mode:

```
Ruijie (dhcp-config) #
```

In this configuration mode, configure the IP address range, the DNS server and the default gateway.

Configuration Examples The following example defines a DHCP address pool named mypool0.

```
ip dhcp pool mypool0
```

Related Commands	Command	Description
	host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	ip dhcp excluded-address	Defines the IP addresses that the DHCP server cannot assign to the clients.
	network (DHCP)	Defines the network number and network mask of the DHCP address pool.

Platform Description N/A

4.28 ip dhcp relay check server-id

Use this command to enable the **ip dhcp relay check server-id** function. Use the **no** form of this command to restore the default setting.

ip dhcp relay check server-id

no ip dhcp relay check server-id

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The **ip dhcp relay check server-id** command is disabled.

Command Mode Global configuration mode.

Usage Guide Switch will select the server to be sent according to server-id option when forwarding DHCP

REQUEST via this command. Without this command configured, the switch forwards the DHCP REQUEST to all configured DHCP servers.

Configuration The following example enables the ip dhcp relay check server-id function.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay check server-id
```

Related Commands	Command	Description
	service dhcp	Enables the DHCP Relay.

Platform N/A

Description

4.29 ip dhcp relay information option82

Use this command to enable the **ip dhcp relay information option82** function. Use the **no** form of this command to restore the default setting.

ip dhcp relay information option82

no ip dhcp relay information option82

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The **ip dhcp relay information option82** command is disabled.

Command Mode Global configuration mode.

Usage Guide When this command is executed, the device serves as the DHCP relay. It adds Option 82 information to DHCP request packets while forwarding these packets.

Configuration The following example enables the option82 function on the DHCP relay.

Examples

```
Ruijie# configure terminal
Ruijie(config)# Ip dhcp relay information option82
```

Related Commands	Command	Description
	service dhcp	Enables the DHCP Relay.

Platform N/A

Description

4.30 ip dhcp relay suppression

Use this command to enable the DHCP binding globally. Use the **no** form of this command to disable the DHCP binding globally and enable the **DHCP relay** suppression on the port.

ip dhcp relay suppression

no ip dhcp relay suppression

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The **ip dhcp relay suppression** command is disabled.

Command Interface configuration mode.

Mode

Usage Guide After executing this command, the system will not relay the DHCP request message on the interface.

Configuration The following example enables the relay suppression function on the interface 1.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp relay suppression
Ruijie(config-if)# exit
Ruijie(config)#
```

Related	Command	Description
Commands	service dhcp	Enables the DHCP Relay.

Platform N/A

Description

4.31 ip dhcp server arp-detect

Use this command to enable the user-offline detection. Use the **no** or **default** form this command to restore the default setting.

ip dhcp server arp-detect

no ip dhcp server arp-detect

default ip dhcp server arp-detect

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to detect whether the user has gone offline. If the user does not go online within a certain period, the IP address is reclaimed.

Configuration Examples The following example enables the user-offline detection.

```
Ruijie(config)# ip dhcp server arp-detect
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.32 ip dhcp server detect

Use this command to enable the fake DHCP server detection. Use the **no** or **default** form of this command to restore the default setting.

ip dhcp server detect

no ip dhcp server detect

default ip dhcp server detect

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this function is enabled, any fake DHCP server detected is logged.

Configuration Examples The following example enables the fake DHCP server detection.

```
Ruijie(config)# ip dhcp server detect
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.33 ip dhcp use class

Use this command to enable the CLASS to allocate addresses in the global configuration mode. Use the **no** form of this command can be used to disable the CLASS.

ip dhcp use class

no ip dhcp use class

Parameter	Parameter	Description
Description	N/A	N/A

Defaults Enabled

Command This function is enabled by default.

Mode

Usage Guide N/A

Configuration The following example enables the CLASS to allocate addresses.

Examples Ruijie(config)# ip dhcp use class

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.34 ip helper-address

Use this command to add an IP address of the DHCP server. Use the **no** form of this command to delete an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

ip helper-address { cycle-mode | [vrf {vrf-name}] A.B.C.D }

no ip helper-address { cycle-mode | [vrf {vrf-name}] A.B.C.D }

Parameter	Parameter	Description
Description	cycle-mode	Forwards all DHCP request packets to all DHCP servers.
	vrf {vrf-name}	Specifies vrf of the server.
	<i>A.B.C.D</i>	Specifies the address of the DHCP server.

Defaults N/A

Command Mode Global configuration mode, interface configuration mode.

Usage Guide Up to 20 DHCP server IP addresses can be configured globally or on a layer-3 interface. One DHCP request of this interface will be sent to these servers. You can select one for confirmation. The global configuration and port-based configuration of the vrf are slightly different. In the global configuration mode, if the vrf is not specified, the default address of the current server does not belong to any vrf. In the port-based configuration, if the vrf is not specified, the current default server and port configurations belong to the same vrf.

Configuration Examples The following example configures the addresses for two servers.

1. Set the IP address for the global server to 192.168.1.1
2. Set the IP address for the vrf instance-based server delp1 to 192.168.2.1

```
Ruijie# configure terminal
Ruijie(config)# ip helper-address 192.168.1.1
Ruijie(config)# ip helper-address vrf dep1 192.168.2.1
```

Related Commands	Command	Description
	service dhcp	Enables the DHCP relay.

Platform Description N/A

4.35 lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting. A limited lease time ranges from 1 minute to 23 hours and 59 minutes.

lease { *days* [*hours*] [*minutes*] | **infinite** }

no lease

default lease

Parameter Description	Parameter	Description
	<i>days</i>	Lease time in days
	<i>hours</i>	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
	<i>minutes</i>	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.
	<i>infinite</i>	Infinite lease time.

Defaults The lease time for a static address pool is infinite. The lease time for other address pools is 1 day.

Command DHCP address pool configuration mode.

Mode

Usage Guide When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.

Configuration The following example sets the DHCP lease to 1 hour.

Examples

```
lease 0 1
```

The following example sets the DHCP lease to 1 minute.

```
lease 0 0 1
```

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.36 lease-threshold

Use this command in DHCP address pool configuration mode to define the DHCP alarm threshold.

Use the **default** or **no** form of this command to restore the default setting.

lease-threshold *percentage*

default lease-threshold

no lease-threshold

Parameter	Parameter	Description
Description	<i>percentage</i>	Usage of the address pool, ranging from 60 to 100 in percentage.

Defaults 90

Command DHCP address pool configuration mode.

Mode

Usage Guide If the maximum IP usage of the address pool reaches the threshold, the DHCP Server generates a SYSLOG alarm. The IP usage indicates the ratio of the number of assigned address pools to the total number of assignable address pools. If the number of assigned pools stays above the alarm threshold, an alarm is generated every 5 minutes.

Configuration The following example sets the alarm threshold to 80%.

Examples

```
lease-threshold 80
```

The following example restores the default alarm threshold.

```
default lease-threshold
```

The following example disables the address pool alarm function.

```
no lease-threshold
```

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.37 match ip

Use this command to define an AM matching rule.

Use the no form of this command to remove the configuration.

Use the clear form of this command to clear all configurations.

match ip *ip-address netmask [interface] [add/remove] vlan vlan-list*

no match ip *ip-address netmask [interface] [add/remove] vlan vlan-list*

clear match ip *[interface]*

Parameter	Parameter	Description
Description	<i>ip-address</i>	IP address
	<i>netmask</i>	Subnet mask
	<i>interface</i>	Interface ID
	<i>add/remove</i>	Adds or removes the specified VLAN.
	<i>vlan-list</i>	VLAN ID

Defaults N/A

Command AM rule configuration mode

Mode

Usage Guide With this function enabled, all DHCP clients with specified *vlan-list* and interface obtain addresses in the rule.

If a DHCP client obtains a static address, it is not subject to AM matching rules in whichever Sub VLAN unless the AM rule configuration is based on VLAN instead of Sub VLAN. This type of matching rules applies to only static addresses.

Configuration The following example defines an AM matching rule.

Examples

```
Ruijie(config-address-manage)#match ip 192.168.11.0 255.255.255.0
GigabitEthernet 0/10 vlan 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.38 match ip default

Use this command to define a default AM matching rule.
 Use the no form of this command to remove the configuration,
match ip default *ip-address netmask*
no match ip default *ip-address netmask*

Parameter	Parameter	Description
Description	<i>ip-address</i>	IP address
	<i>netmask</i>	Subnet mask

Defaults N/A

Command Mode AM rule configuration mode

Usage Guide With this function enabled, all DHCP clients with specified vlan-list and interface obtain addresses in the default rule.

Configuration Examples The following example defines a default AM matching rule.

```
Ruijie(config-address-manage)#match ip default 192.168.12.0 255.255.255.0
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.39 netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The **no** form of this command can be used to restore the default setting.

netbios-name-server *ip-address [ip-address2...ip-address8]*
no netbios-name-server
default netbios-name-server

Parameter	Parameter	Description
Description	<i>ip-address</i>	IP address of the WINS server. It is required to configure one IP address at least.

<i>ip-address2...ip-address8</i>	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.
----------------------------------	--

Defaults No WINS server is defined by default.

Command DHCP address pool configuration mode.

Mode

Usage Guide When more than one WINS server is defined, the former has higher priority. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

Configuration The following example specifies the WINS server 192.168.12.3 for the DHCP client.

Examples

```
netbios-name-server 192.168.12.3
```

Related	Command	Description
Commands	ip address dhcp	Enables the DHCP client on the interface to obtain the IP address.
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	netbios-node-type	Defines the netbios node type of the client host.

Platform N/A

Description

4.40 netbios-node-type

Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. Use the **no** or **default** form of this command to restore the default setting.

netbios-node-type *type*

no netbios-node-type

default netbios-node-type

Parameter	Parameter	Description
Description	<i>type</i>	Type of node in two modes: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: 1: b-node. 2: p-node. 4: m-node. 8: h-node. String: b-node: broadcast node p-node: peer-to-peer node

	m-node: mixed node h-node: hybrid node
--	---

Defaults No type of the NetBIOS node is defined by default.

Command DHCP address pool configuration mode.

Mode

Usage Guide There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received.

By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.

Configuration The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

Examples `netbios-node-type h-node`

Related	Command	Description
Commands	<code>ip dhcp pool</code>	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.
	<code>netbios-name-server</code>	Configures the WINS name server of the Microsoft DHCP client NETBIOS.

Platform N/A

Description

4.41 network (DHCP)

Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

network *network-number net-mask* [*low-ip-address high-ip-address*]

no network

default network

Parameter	Parameter	Description
Description	<i>net-number</i>	Network number of the DHCP address pool
	<i>net-mask</i>	Network mask of the DHCP address pool. If the network mask is not

	defined, the natural network mask will be used by default.
low-ip-address	Available start IP address
high-ip-address	Available end IP address

Defaults No network number or network mask is defined by default.

Command DHCP address pool configuration mode.

Mode

Usage Guide This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address.

The **show ip dhcp binding** command can be used to view the address assignment, and the **show ip dhcp conflict** command can be used to view the address conflict detection configuration.

Configuration Examples The following example defines the network number of the DHCP address pool as 192.168.12.0, and the network mask as 255.255.255.240.

```
network 192.168.12.0 255.255.255.240
```

Related Commands	Command	Description
	ip dhcp excluded-address	Defines the IP addresses that the DHCP server cannot assign to the clients.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.42 next-server

Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. Use the **no** or **default** form of this command to restore the default setting.

next-server *ip-address* [*ip-address2*...*ip-address8*]

no next-server

default next-server

Parameter Description	Parameter	Description
	<i>ip-address</i>	Defines the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.

<i>ip-address2...ip-address8</i>	(Optional) Up to 8 startup servers can be configured.
----------------------------------	---

Defaults N/A

Command Mode DHCP address pool configuration mode.

Usage Guide When more than one startup server is defined, the former will possess higher priority. The DHCP client will select the next startup server only when its communication with the former startup server fails.

Configuration Examples The following example specifies the startup server 192.168.12.4 for the DHCP client.

```
next-server 192.168.12.4
```

Related Commands	Command	Description
	bootfile	Defines the default startup mapping file name of the DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	ip help-address	Defines the Helper address on the interface.
	option	Configures the option of the RGOS software DHCP server.

Platform N/A

Description

4.43 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

no option

default option

Parameter Description	Parameter	Description
	<i>code</i>	Defines the DHCP option codes.
	ascii <i>string</i>	Defines an ASCII string.
	hex <i>string</i>	Defines a hex string.
	ip <i>ip-address</i>	Defines an IP address list.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.

Configuration Examples The following example defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client.

```
Ruijie(dhcp-config)# option 19 hex 1
```

The following example defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway 192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16.

```
option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0 192.168.12.16
```

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A
Description

4.44 pool-status

Use this command to enable or disable the DHCP address pool.

```
pool-status { enable | disable }
```

Parameter Description	Parameter	Description
	enable	Enables the address pool.
	disable	Disables the address pool.

Defaults By default, the address pool is enabled after it is configured.

Command Mode DHCP address pool configuration mode

Usage Guide This command is configured on the DHCP server.

Configuration Examples The following example disables the address pool.

```
Ruijie(dhcp-config)# pool-status disable
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

4.45 relay agent information

Use this command to enter the Option82 matching information configuration mode in the global CLASS configuration mode. Use the **no** form of this command to delete the Option82 matching information of the CLASS.

relay agent information

no relay agent information

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Global CLASS configuration mode

Usage Guide After executing this command, it enters the Option82 matching information configuration mode which is shown as "Ruijie (config-dhcp-class-relayinfo)#".
 In this configuration mode, user can configure the class matching multiple Option82 information.

Configuration Examples The following example configures a global CLASS and enters the Option82 matching information configuration mode.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)#
```

Related	Command	Description
Commands	ip dhcp class	Defines a CLASS and enters the global CLASS configuration mode.

Platform N/A
Description

4.46 relay-information hex

Use this command to enter the Option82 matching information configuration mode. Use the **no** form of this command to delete a piece of matching information.

relay-information hex aabb.ccdd.eeff... [*]
no relay-information hex aabb.ccdd.eeff... [*]

Parameter	Parameter	Description
Description	aabb.ccdd.eeff...[*]	Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching.

Defaults N/A

Command Mode Global CLASS configuration mode

Usage Guide N/A

Configuration Examples The following example configures a global CLASS which can match multiple Option82 information.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)# relay-information
hex 0102256535
Ruijie(config-dhcp-class-relayinfo)# relay-information
hex 010225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information
hex 060225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information
hex 060223*
```

Related Commands	Command	Description
	ip dhcp class	Defines a CLASS and enter the global CLASS configuration mode.
	relay agent information	Enters the Option82 matching information configuration mode.

Platform Description N/A

4.47 remark

Use this command to configure the identification which is used to describe the CLASS in this global CLASS configuration mode. Use the **no** form of this command to delete the identification.

remark class-remark
no remark

Parameter	Parameter	Description
Description	class-remark	Information used to identify the CLASS, which can be the character

	strings with space in them.
--	-----------------------------

Defaults N/A.

Command Mode Global CLASS configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the identification information for a global CLASS.

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# remark used in #1 build
```

Related Commands	Command	Description
	ip dhcp class	Defines a CLASS and enter the global CLASS configuration mode.

Platform Description N/A

4.48 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

- service dhcp**
- no service dhcp**
- default service dhcp**

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The **service dhcp** command is disabled.

Command Mode Global configuration mode

Usage Guide The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.

Configuration Examples The following example enables the DHCP server and the DHCP relay feature.

```
service dhcp
```

Related Commands	Command	Description
	<code>show ip dhcp server statistics</code>	Displays various statistics information of the DHCP server.
	<code>ip helper-address [vrf] A.B.C.D</code>	Adds an IP address of the DHCP server.

Platform N/A
Description

4.49 show dhcp exclude

Use this command to display the excluded address.

show dhcp exclude

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the excluded address.

```

Examples
Ruijie(config)#sh dhcp ex
low          high
-----
20.1.1.1     20.1.1.2
30.1.1.1     30.1.1.20
Ruijie(config)#
    
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.50 show dhcp lease

Use this command to display the lease information of the IP address obtained by the DHCP client.

show dhcp lease

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide If the IP address is not defined, display the binding condition of all addresses. If the IP address is defined, display the binding condition of this IP address.

Configuration Examples The following example displays the result of the show dhcp lease.

```
Ruijie# show dhcp lease
Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0
Temp sub net mask: 255.255.255.0
  DHCP Lease server: 192.168.5.70, state: 3 Bound
  DHCP transaction id: 168F
  Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
  Next timer fires after: 00:04:29
  Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Fa0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.51 show dhcp manual-bind

Use this command to display the binding address.

show dhcp manual-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the binding address.

```
Ruijie# show dhcp manual-bind
ip          mask          uid/mac          pool_name        gateway          dns
```


20.1.1.122 255.0.0.0 0000.0000.0001 static1 1.1.1.1	
2.2.2.2	
ip	IP address
mask	Subnet mask
uid/mac	UID/MAC address
Pool name	Address pool name
gateway	Gateway
dns	DNS server name

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.52 show dhcp name

Use this command to display all DHCP address pool names.

show dhcp name

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays all DHCP address pool names.

Examples

```
Ruijie(dhcp-config)#sho dhcp name
DYNAMIC POOL
pool name:net20

MANUAL POOL
pool name:static1
pool name:static2
```

```
UNKNOWN POOL
pool name:test
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.53 show dhcp pool

Use this command to display the configuration of a specified address pool.

show dhcp pool *name*

Parameter Description	Parameter	Description
	<i>name</i>	Specifies the address pool.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of a specified address pool.

```
Ruijie(dhcp-config)#show dhcp pool net20
network : 20.0.0.0
netmask : 255.0.0.0
lease-infinite : false
lease-days : 1
lease-hours : 0
lease-minutes : 0
netbios-type : 0
domain-name :
gateway :
dns:
ntp:
option-43:
option-138:
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.54 show dhcp state

Use this command to display whether DHCP server is enabled.

show dhcp state

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays whether DHCP server is enabled.

Examples

```
Ruijie#show dhcp state
dhcp-server state : true
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.55 show ip dhcp binding

Use this command to display the binding condition of the DHCP address.

show ip dhcp binding [ip-address]

Parameter	Parameter	Description
Description	<i>ip-address</i>	(Optional) Only displays the binding condition of the specified IP addresses.

Defaults N/A

Command Privileged EXEC mode.

Mode

Usage Guide If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address

Configuration The following is the result of the show ip dhcp binding.

Examples

```
Ruijie# show ip dhcp binding
Total number of clients   : 4
Expired clients           : 3
Running clients           : 1

IP address      Hardware address      Lease expiration      Type
20.1.1.1       2000.0000.2011      000 days 23 hours 59 mins  Automatic
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	The IP address to be assigned to the DHCP client.
Client-Identifier /Hardware address	The client identifier or hardware address of the DHCP client.
Lease expiration	The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively.
Type	The type of the address binding. The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual.

**Related
Commands**

Command	Description
clear ip dhcp binding	Clears the DHCP address binding table.

Platform N/A

Description

4.56 show ip dhcp conflict

Use this command to show the conflict history record of the DHCP sever.

show ip dhcp conflict

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode.

Mode

Usage Guide This command can display the conflict address list detected by the DHCP server.

Configuration The following example displays the output result of the **show ip dhcp conflict** command.

Examples

```
Ruijie# show ip dhcp conflict
IP address  Detection Method
192.168.12.1 Ping
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	The IP addresses which cannot be assigned to the DHCP client.
Detection Method	The conflict detection method.

Related**Commands**

Command	Description
clear ip dhcp conflict	Clears the DHCP conflict record.

Platform N/A

Description

4.57 show ip dhcp history

Use this command to display the DHCP lease history.

show ip dhcp history

Parameter**Description**

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide This command is configured on the DHCP server.

Configuration The following example displays the DHCP lease history.

Examples

```
Ruijie#show ip dhcp history
Expired clients          : 3
IP address              Hardware address      Lease expiration        Vlan/Relay
10.1.1.5                 2222.abcd.47ac          IDLE                    4097
10.1.1.4                 2222.abcd.47ae          IDLE                    4097
10.1.1.3                 2222.abcd.47ad          IDLE                    4097
```

```
Running clients      : 0
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.58 show ip dhcp identifier

Use this command to display the DHCP address pool ID and address usage.

show ip dhcp identifier

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the DHCP address pool ID and address usage.

```
Ruijie# show ip dhcp identifier
```

```
Pool name      Identifier      Total      Distributed  Remained
-----
wzp            597455782      65533      0            65533
```

Pool name	Address pool name.
Identifier	Address pool ID.
Total	Total number of addresses.
Distributed	Number of allocated addresses.
Remained	Number of remained addresses.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.59 show ip dhcp pool

Use this command to display the address statistics of an address pool.

show ip dhcp pool [*poolname*]

Parameter	Parameter	Description
Description	<i>poolname</i>	(Optional) Address pool whose address statistics are to be displayed.

Defaults Privileged EXEC mode.

Command Mode N/A

Usage Guide Use this command to show the address statistics of an address pool.

Configuration Examples The following example displays the output result of the **show ip dhcp pool** *poolname* command.

```
Ruijie# show ip dhcp poolname
Pool poolname:
  Address range      192.168.0.1 - 192.168.0.254
  Class range       192.168.0.1 - 192.168.0.254
  Total address     252
  Excluded          2
  Distributed       30
  Conflict          10
  Remained          212
  Usage percentage  84.12698%
  Lease threshold   90%
```

The meaning of various fields in the show result is described as follows.

Field	Description
Address range	Address range of the address pool.
Class range	Class address range. By default, the address range for the same address pool is not configured. Otherwise, the class range is displayed.
Total address	Total number of addresses that can be assigned in the address pool.
Excluded	Number of excluded addresses.
Distributed	Number of assigned addresses.
Conflict	Number of conflicting addresses in the address pool.
Remained	Number of remaining addresses that have not been assigned or can be reused.
Usage percentage	Address pool usage.
Lease threshold	Lease threshold.

Related	Command	Description
Commands	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform N/A

Description

4.60 show ip dhcp relay-statistics

Use this command to display the statistics of the DHCP relay.

show ip dhcp relay-statistics

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide This command is used to display the statistics of the DHCP relay.

Configuration The following example displays the statistics of the DHCP relay.

Examples Ruijie# show ip dhcp relay-statistics

```

Cycle mode                0

Message                   Count
Discover                  0
Offer                     0
Request                   0
Ack                       0
Nak                       0
Decline                   0
Release                   0
Info                      0
Bad                       0

Direction                 Count
Rx client                 0
Rx client uni             0
Rx client bro             0
Tx client                 0
Tx client uni             0

```



```
Tx client bro      0
Rx server         0
Tx server         0
```

The meaning of various fields in the show result is described as follows.

Field	Description
Cycle mode	Whether to allow packets to be sent to multiple DHCP servers.
Discover	The number of Discover packets.
Offer	The number of Offer packets.
Request	The number of Request packets.
Ack	The number of Ack packets.
Nak	The number of Nak packets.
Decline	The number of Decline packets.
Release	The number of Release packets.
Info	The number of Info packets.
Bad	The number of error packets.
Rx client	The number of packets received from the client.
Rx client uni	The number of unicast packets received from the client.
Rx client bro	The number of broadcast packets received from the client.
Tx client	The number of packets transmitted to the client.
Tx client uni	The number of unicast packets transmitted to the client
Tx client bro	The number of multicast packets transmitted to the client
Rx server	The number of packets received from the server.
Tx server	The number of packets transmitted to the server.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.61 show ip dhcp server detect

Use this command to display the fake DHCP server detected.

show ip dhcp server detect

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the fake DHCP server detected.

Examples

```
Ruijie#show ip dhcp server detect
The DHCP Server information:
Server IP = 10.1.10.40, DHCP server interface = GigabitEthernet 0/1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.62 show ip dhcp server statistics

Use this command to display the statistics of the DHCP server.

show ip dhcp server statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the statistics of the DHCP server.

Configuration Examples The following example displays the output result of the **show ip dhcp server statistics** command.

Examples

```
Ruijie# show ip dhcp server statistics
Address pools          2
Lease counter         4
Active Lease Counter  0
Expired Lease Counter 4
Malformed messages    0
Dropped messages      0
```

```

Message                Received
BOOTREQUEST            216
DHCPDISCOVER           33
DHCPREQUEST            25
DHCPDECLINE            0
DHCPRELEASE            1
DHCPINFORM             150

Message                Sent
BOOTREPLY              16
DHCPOFFER              9
DHCPACK                7
DHCPNAK                0
DHCPREQUESTS          0
DHCPREQUESTSUC        0
DISCOVER-PROCESS-ERROR 0
LEASE-IN-PINGSTATE    0
NO-LEASE-RESOURCE     0
SERVERID-NO-MATCH     0
-----
rcv                    0
send                   0
    
```

The meaning of various fields in the show result is described as follows.

Field	Description
Address pools	Number of address pools.
Lease count	Number of allocated lease.
Automatic bindings	Number of automatic address bindings.
Manual bindings	Number of manual address bindings.
Expired bindings	Number of expired address bindings.
Malformed messages	Number of malformed messages received by the DHCP.
Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.

Related Commands	Command	Description
	clear ip dhcp server statistics	Clears the DHCP server statistics.

Platform N/A
Description

4.63 show ip dhcp socket

Use this command to display the socket used by the DHCP server.

show ip dhcp socket

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the socket used by the DHCP server.

Examples

```
ruijie#show ip dhcp socket
dhcp socket = 47.
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5 DHCPv6 Commands

5.1 clear ipv6 dhcp binding

Use this command to clear the DHCPv6 binding information.

clear ipv6 dhcp binding [*ipv6-address*]

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the IPv6 address or the prefix.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *ipv6-address* is not specified, all DHCPv6 binding information is cleared. If the *ipv6-address* is specified, the binding information for the specified address is cleared.

Configuration Examples The following example clears the DHCPv6 binding information:

```
Ruijie(config)# clear ipv6 dhcp binding
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.2 clear ipv6 dhcp conflict

Use this command to clear the DHCPv6 address conflicts.

clear ipv6 dhcp conflict { *ipv6-address* | * }

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Specifies IPv6 address or prefix.
	*	All IPv6 addresses or prefixes

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If an IPv6 address conflict is detected, the DHCPv6 client will send the Decline message. Then the DHCPv6 server will add the address in this message into the address conflict queue. The addresses added into the address conflict queue cannot be assigned any longer.
 If the * parameter is not specified, all conflicts of IPv6 addresses or prefixes will be deleted.
 If the *ipv6-address* parameter is specified, only the specified address conflict will be deleted.

Configuration The following example clears a DHCPv6 address conflict.

Examples

```
Ruijie# clear ipv6 dhcp conflict 2008:50::2
```

Related	Command	Description
Commands	show ipv6 dhcp conflict	Displays address conflicts.

Platform N/A
Description

5.3 clear ipv6 dhcp relay statistics

Use this command to clear the packet sending and receiving condition with the DHCPv6 Relay function enabled.

clear ipv6 dhcp relay statistics

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears the packet sending and receiving condition with the DHCPv6 Relay function enabled.

```
Ruijie# clear ipv6 dhcp relay statistics
```

Related	Command	Description
Commands	show ipv6 dhcp relay statistics	Displays the statistical information.

Platform N/A
Description

5.4 clear ipv6 dhcp server statistics

Use this command to clear the DHCPv6 server statistics.

clear ipv6 dhcp server statistics

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the DHCPv6 server statistics.

Configuration The following example clears the DHCPv6 server statistics.

Examples Ruijie(config)# clear ipv6 dhcp server statistics

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

5.5 dns-server

Use this command to set the DNS Server list information for the DHCPv6 Server.

Use the **no** form of this command to restore the default setting.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the IPv6 address or the DNS server.

Defaults By default, no DNS server list is configured.

Command Mode DHCPv6 pool configuration mode

Usage Guide To configure several DNS Server addresses, use the **dns-server** command for several times. The newly-configured DNS Server address will not overwrite the former ones.

Configuration The following example configures the DNS server address.

Examples

```
Ruijie(config-dhcp)# dns-server 2008:1::1
```

Related Commands	Command	Description
	domain-name	Sets the DHCPv6 domain name information.
	ipv6 dhcp pool	Sets a DHCPv6 pool.

Platform N/A

Description

5.6 domain-name

Use this command to set the domain name for the DHCPv6 server.

Use the **no** form of this command to restore the default setting.

domain-name *domain*

no domain-name *domain*

Parameter	Parameter	Description
Description	<i>domain</i>	Sets the domain name.

Defaults By default, no domain name is configured.

Command DHCPv6 pool configuration mode

Mode

Usage Guide To configure several domain names, use the domain-name command for several times. The newly-configured domain name will not overwrite the former ones.

Configuration The following example sets the domain name for the DHCPv6 server to example.com.

Examples

```
Ruijie(config-dhcp)# domain-name example.com
```

Related Commands	Command	Description
	dns-server	Sets the DHCPv6 DNS server list.
	ipv6 dhcp pool	Sets the DHCPv6 pool.

Platform N/A

Description

5.7 iana-address prefix

Use this command to set the IA_NA address prefix for the DHCPv6 Server. Use the **no** form of this command to restore the default setting.

iana-address prefix *ipv6-prefix/prefix-length* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]

no iana-address prefix

Parameter	Parameter	Description
Description	<i>ipv6-prefix/prefix-length</i>	Sets the IPv6 prefix and prefix length.
	lifetime	Sets the lifetime of the address allocated to the client. With the keyword lifetime configured, both parameters <i>valid-lifetime</i> and <i>preferred-lifetime</i> shall be configured.
	<i>valid-lifetime</i>	Sets the valid lifetime of using the allocated address for the client.
	<i>preferred-lifetime</i>	Sets the preferred lifetime of the address allocated to the client.

Defaults By default, no IA_NA address prefix is configured.
The default *valid-lifetime* is 3600s(1 hour).
The default *preferred-lifetime* is 3600s(1 hour).

Command Mode DHCPv6 pool configuration mode

Usage Guide This command is used to set the IA_NA address prefix for the DHCPv6 Server, and allocate the IA_NA address to the client.
The Server attempts to allocate a usable address within the IA_NA address prefix range to the client upon receiving the IA_NA address request from the client. That address will be allocated to other clients if the client no longer uses that address again.

Configuration Examples The following example sets the IA_NA address prefix for the DHCPv6 Server.

```
Ruijie(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000
1000Ruijie(config-if)# ip verify urpf drop-rate notify
```

Related Commands	Command	Description
	ipv6 dhcp pool	Sets the DHCPv6 pool.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.8 ipv6 dhcp pool

Use this command to set the DHCPv6 server pool.
Use the **no** form of this command to restore the default setting.

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Parameter	Parameter	Description
Description	<i>poolname</i>	Defines the DHCPv6 pool name.

Defaults By default, no DHCPv6 server pool is configured.

Command Mode Global configuration mode

Usage Guide This command is used to create a DHCPv6 Server configuration pool. After configuring this command, it enters the DHCPv6 pool configuration mode, in which the administrator can set the pool parameters, such as the prefix and the DNS Server information, ect.
 After creating the DHCPv6 Server configuration pool, use the **ipv6 dhcp server** command to associate the pool and the DHCPv6 Server on one interface.

Configuration The following example sets the DHCPv6 server pool.

```
Examples Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp pool pool1
Ruijie(config-dhcp)#
```

Related Commands	Command	Description
	ipv6 dhcp server	Enables the DHCPv6 server function on the interface.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.9 ipv6 dhcp relay destination

Use this command to enable the DHCPv6 relay service and configure the destination address to which the messages are forwarded.

Use the **no** form of this command to restore the default setting.

ipv6 dhcp relay destination*ipv6-address* [*interface-type interface-number*]

no ipv6 dhcp relay destination*ipv6-address* [*interface-type interface-number*]

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the DHCPv6 relay destination address.
	<i>interface-type</i>	Specifies the forwarding output interface if the forwarding address is the local link address.
	<i>interface-number</i>	

Defaults By default, the relay and forward function is disabled, and the forwarding destination address and the output interface are not configured.

Command Mode Interface configuration mode

Usage Guide With the DHCPv6 relay service enabled on the interface, the DHCPv6 message received on the interface can be forwarded to all configured destination addresses. Those received DHCPv6 messages can be from the client, or from another DHCPv6 relay service.

The forwarding output interface configuration is mandatory if the forwarding address is the local link address or the multicast address. And the forwarding output interface configuration is optional if the forwarding address is global or station unicast or multicast address.

Without the forwarding output interface configured, the interface is selected according to the unicast or multicast routing protocol.

The relay reply message can be forwarded without the relay function enabled on the interface.

Configuration The following example sets the relay destination address on the interface.

Examples

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp relay destination 2008:1::1
```

Related	Command	Description
Commands	show ipv6 dhcp interface	Displays the DHCPv6 interface information.

Platform N/A
Description

5.10 ipv6 dhcp server

Use this command to enable the DHCPv6 server on the interface.

Use the **no** form of this command to restore the default setting.

ipv6 dhcp server *poolname* [**rapid-commit] [**preference** *value*]**
no ipv6 dhcp server

Parameter	Parameter	Description
Description	<i>poolname</i>	Defines the DHCPv6 pool name.
	rapid-commit	Allows the two-message interaction process.
	preference <i>value</i>	Sets the preference level for the advertise message. The valid range is from 1 to 100 and the default value is 0.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use the **ipv6 dhcp server** command to enable the DHCPv6 service.

Configuring the keyword **rapid-commit** allows the two-message interaction for the server and the client when allocating the address prefix and setting other configurations. With this keyword configured, if the client solicit message includes the **rapid-commit** item, the DHCPv6 Server will send

the Reply message immediately.

DHCPv6 Server carries with the **preference** value when sending the advertise message if the **preference** level is not 0.

If the **preference** level is 0, the advertise message will not include this field. If the **preference** value is 255, the client sends the request message to the server to obtain the configurations.

DHCPv6 Client, Server and Relay functions are exclusive, and only one of the functions can be configured on the interface.

Configuration The following example enables the DHCPv6 server on the interface.

Examples

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp server pool1
```

Related Commands	Command	Description
	ipv6 dhcp pool	Sets the DHCPv6 pool.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform N/A

Description

5.11 ipv6 local pool

Use this command to configure the local prefix pool of the DHCPv6 server prefix.

Use the **no** form of this command to restore the default setting.

ipv6 local pool *poolname prefix/prefix-length assigned-length*

no ipv6 local pool *poolname*

Parameter Description	Parameter	Description
	<i>poolname</i>	The local prefix pool name
	<i>prefix/prefix-length</i>	The prefix and prefix length
	<i>assigned-length</i>	The assigned prefix length

Defaults By default, no local prefix pool of the DHCPv6 server prefix is configured.

Command Mode Global configuration mode

Usage Guide The **ipv6 local pool** command is used to create the local prefix pool. If the DHCPv6 server requires prefix delegation, you can use the **prefix-delegation pool** command to specify the local prefix pool and then assign prefixes from the prefix pool.

Configuration The following example configures the local prefix pool.

Examples

```
Ruijie(config)# ipv6 local pool client-prefix-pool 2001::db8::/64 80
```

The following example specifies the local prefix pool.

```
Ruijie(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000
1000
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

5.12 option52

Use this command to configure the DHCPv6 Server to set the CAPWAP AC IPv6 address.
Use the **no** form of this command to restore the default setting.

option52 *ipv6-address*

no option52 *ipv6-address*

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the CAPWAP AC IPv6 address.

Defaults By default, no option52 is created after pool configuration on the DHCPv6 server is complete.

Command Mode DHCPv6 pool configuration mode

Usage Guide This command can be used to set multiple CAPWAP AC IPv6 addresses. The newly added IPv6 address does not overwrite the old one.

Configuration Examples The following example configures the domain-name address.

```
Ruijie(config-dhcp)# option52 2008:1::1
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

5.13 prefix-delegation

Use this command to set the static binding address prefix information for the DHCPv6 server.
Use the **no** form of this command to restore the default setting.

prefix-delegation *ipv6-prefix/prefix-length client-DUID [lifetime]*

no prefix-delegation *ipv6-prefix/prefix-length client-DUID [lifetime]*

Parameter	Parameter	Description
Description	<i>ipv6-prefix/prefix-length</i>	Sets the IPv6 address prefix and the prefix length.
	<i>client-DUID</i>	Sets the client DUID.
	<i>lifetime</i>	Sets the interval of using the prefix by the client.

Defaults By default, no address prefix information is configured.
The default *lifetime* is 3600 seconds (one hour).

Command Mode DHCPv6 pool configuration mode

Usage Guide The administrator uses this command to manually set the address prefix information list for the client IA_PD and set the valid lifetime for those prefixes.
The parameter *client-DUID* allocates the address prefix to the first IA_PD in the specified client.
Before receiving the request message for the address prefix from the client, DHCPv6 Server searches for the corresponding static binding first. If it succeeds, the server returns to the static binding; otherwise, the server will attempt to allocate the address prefix from other prefix information sources.

Configuration Examples Ruijie (config-dhcp) # `prefix-delegation 2008:2::/64 0003000100d0f82233ac`

Related Commands	Command	Description
	ipv6 dhcp pool	Sets a DHCPv6 pool.
	ipv6 local pool	Sets a local prefix pool.
	prefix-delegation pool	Specifies the DHCPv6 local prefix pool.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform Description N/A

5.14 prefix-delegation pool

Use this command to specify the local prefix pool for the DHCPv6 server.
Use the **no** form of this command to restore the default setting.

prefix-delegation pool *poolname* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]
no prefix-delegation pool *poolname*

Parameter	Parameter	Description
Description	<i>poolname</i>	Sets the local prefix pool name.
	lifetime	Sets the lifetime of the address prefix allocated to the client. With the keyword lifetime configured, both parameters <i>valid-lifetime</i> and <i>preferred-lifetime</i> shall be configured.

<i>valid-lifetime</i>	Sets the valid lifetime of using the allocated address prefix for the client.
<i>preferred-lifetime</i>	Sets the preferred lifetime of the address prefix allocated to the client.

Defaults By default, no address prefix pool is specified.
The default *valid-lifetime* is 3600s(1 hour).
The default *preferred-lifetime* is 3600s(1 hour).

Command Mode DHCPv6 pool configuration mode

Usage Guide Use the **prefix-delegation pool** command to set the prefix pool for the DHCPv6 Server and allocate the prefix to the client. Use the **ipv6 local pool** command to set the prefix pool.
The Server attempts to allocate a usable prefix from the prefix pool to the client upon receiving the prefix request from the client. That prefix will be allocated to other clients if the client no longer uses that prefix again.

Configuration The following example specifies the local prefix pool for the DHCPv6 server.

Examples

```
Ruijie (config-dhcp) # prefix-delegation pool client-prefix-pool lifetime 2000
1000
```

Related Commands	Command	Description
	ipv6 dhcp pool	Sets a DHCPv6 pool.
	ipv6 local pool	Sets a local prefix pool.
	prefix-delegation	Statically binds the client with the address prefix.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.

Platform N/A
Description

5.15 show ipv6 dhcp

Use this command to display the device DUID.

show ipv6 dhcp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Interface configuration mode/Global configuration mode

Usage Guide The server, client and relay on the same device share a DUID.

Configuration The following example displays the device DUID.

Examples

```
Ruijie# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.16 show ipv6 dhcp binding

Use this command to display the address binding information for the DHCPv6 server.

show ipv6 dhcp binding [*ipv6-address*]

Parameter Description	Parameter	Description
	<i>ipv6-address</i>	Sets the IPv6 address or the prefix.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *ipv6-address* is not specified, all prefixes dynamically assigned to the client and IANA address binding information are shown. If the *ipv6-address* is specified, the binding information for the specified address is shown.

Configuration The following example displays the address binding information for the DHCPv6 server.

Examples

```
Ruijie# show ipv6 dhcp binding
Client DUID: 00:03:00:01:00:d0:f8:22:33:ac
  IAPD: iaid 0, T1 1800, T2 2880
  Prefix: 2001:20::/72
         preferred lifetime 3600, valid lifetime 3600
         expires at Jan 1 2008 2:23 (3600 seconds)
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.17 show ipv6 dhcp conflict

Use this command to display the DHCPv6 address conflicts.

show ipv6 dhcp conflict

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the DHCPv6 address conflicts.

Examples Ruijie# show ipv6 dhcp conflict

```
2008:50::2    declined
2108:50::2    declined
2008:50::3    declined
2008:50::4    declined
2108:50::4    declined
2008:50::5    declined
```

Related Commands	Command	Description
	clear ipv6 dhcp conflict	Clears address conflicts.

Platform N/A

Description

5.18 show ipv6 dhcp interface

Use this command to display the DHCPv6 interface information.

show ipv6 dhcp interface [*interface-name*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Sets the interface name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *interface-name* is not specified, all DHCPv6 interface information is displayed. If the *interface-name* is specified, the specified interface information is displayed.

Configuration The following example displays the DHCPv6 interface information.

Examples

```
Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool dhcp-pool
  Rapid-Commit: disable
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

5.19 show ipv6 dhcp pool

Use this command to display the DHCPv6 pool information.

show ipv6 dhcp pool [*poolname*]

Parameter	Parameter	Description
Description	<i>poolname</i>	Defines the DHCPv6 pool name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the *poolname* is not specified, all DHCPv6 interface information is displayed. If the *poolname* is specified, the specified interface information is displayed.

Configuration The following example displays the DHCPv6 pool information.

Examples

```
Ruijie# show ipv6 dhcp pool
DHCPv6 pool: dhcp-pool
  DNS server: 2011:1::1
  DNS server: 2011:1::2
  Domain name: example.com
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

5.20 show ipv6 dhcp relay destination

Use this command to display the destination information about DHCPv6 Relay Agent.

show ipv6 dhcp relay destination { *all* | *interface-type interface-number* }

Parameter	Parameter	Description
description	all	Displays information about all configured destination addresses and relay exits.
	interface <i>interface-type</i> <i>interface-number</i>	Displays the relay destination address and relay exit configured for a specified interface.

Defaults N/A

Command mode Privileged EXEC mode

Usage guideline Use this command to show the relay destination address to which DHCPv6 packets sent from a client are forwarded through a specified relay exit (optional) by an interface for which the relay function has been enabled by Relay Agent.

Examples The following example displays all the relay destination addresses.

```
Ruijie# show ipv6 dhcp relay destination all
Interface: Vlan1 //interface for which the relay function has been enabled
Destination address(es)                               Output Interface
3001::2
FF02::1:2 //specified destination address             Vlan2 //specified
relay exit
```

Related commands	Command	Description
	N/A	N/A

Platform description N/A

5.21 show ipv6 dhcp relay statistics

Use this command to display the packet sending and receiving condition with the DHCPv6 Relay function enabled.

show ipv6 dhcp relay statistics

Parameter	Parameter	Description
Description	N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide N/A.

Configuration Examples The following example displays the packet sending and receiving condition with the DHCPv6 Relay function enabled.

```
Ruijie# show ipv6 dhcp relay statistics
Packets dropped          : 2
  Error                  : 2
  Excess of rate limit   : 0
Packets received        : 28
  SOLICIT                : 0
  REQUEST                : 0
  CONFIRM                : 0
  RENEW                  : 0
  REBIND                 : 0
  RELEASE                 : 0
  DECLINE                : 0
  INFORMATION-REQUEST    : 14
  RELAY-FORWARD          : 0
  RELAY-REPLY            : 14
Packets sent            : 16
  ADVERTISE              : 0
  RECONFIGURE            : 0
  REPLY                  : 8
  RELAY-FORWARD          : 8
  RELAY-REPLY            : 0
```

Related Commands	Command	Description
	clear ipv6 dhcp relay statistics	Clears the statistical information.

Platform Description N/A

5.22 show ipv6 dhcp server statistics

Use this command to display the DHCPv6 server statistics.

show ipv6 dhcp server statistics

Parameter	Parameter	Description
-----------	-----------	-------------

Description	N/A	N/A
--------------------	-----	-----

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the DHCPv6 server statistics.

Configuration The following example displays the DHCPv6 server statistics.

Examples Ruijie# show ipv6 dhcp server statistics

```
DHCPv6 server statistics:

Packet statistics:
DHCPv6 packets received:          7
Solicit received:                  7
Request received:                  0
Confirm received:                  0
Renew received:                    0
Rebind received:                   0
Release received:                  0
Decline received:                  0
Relay-forward received:            0
Information-request received:      0
Unknown message type received:     0
Error message received:            0

DHCPv6 packet sent:               0
Advertise sent:                    0
Reply sent:                         0
Relay-reply sent:                  0
Send reply error:                  0
Send packet error:                 0

Binding statistics:
Bindings generated:                0
IAPD assigned:                     0
IANA assigned:                     0

Configuration statistics:
DHCPv6 server interface:           1
DHCPv6 pool:                       0
DHCPv6 iapd binding:               0
```

Related Commands	Command	Description
	ipv6 dhcp pool	Sets a DHCPv6 pool.

Platform N/A

Description

5.23 show ipv6 local pool

Use this command to display the local prefix pool configuration and usage.

show ipv6 local pool [*poolname*]

Parameter Description	Parameter	Description
	<i>poolname</i>	The local prefix pool name

Defaults N/A

Command Mode Privileged EXEC mode

Mode

Usage Guide This command is used to display the local prefix pool configuration and usage.

Configuration Examples The following example displays all local prefix pool information.

Examples

```
Ruijie#show ipv6 local pool
Pool                               Prefix
Free           In use
client-prefix-pool                2001:db8::/64
65536           0
```

Field	Description
Pool	The local address pool name.
Prefix	The prefix and prefix length.
Free	The available prefix.
In use	The prefix in use.

The following example displays the information about the specified local prefix pool.

```
Ruijie#show ipv6 local pool client-prefix-pool
Prefix is 2001:db8::/64 assign /80 prefix
1 entries in use, 65535 available
Prefix                               Interface
2001:db8::/80                        GigabitEthernet 0/0
```

Filed	Description
Prefix	The assigned prefix and prefix length.
Interface	The assigning interface.

Related	Command	Description
---------	---------	-------------

Commands	N/A	N/A
-----------------	-----	-----

Platform N/A

Description

6 DNS Commands

6.1 clear host

Use this command to clear the dynamically learned host name.

clear host [* | *host-name*]

Parameter Description	Parameter	Description
	<i>host-name</i>	Deletes the specified dynamic domain name buffer.
	*	Deletes all dynamic domain name buffer.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.

Configuration Examples The following configuration deletes the dynamically learned mapping records from the host name-IP address buffer table.

```
Ruijie(config)#clear host *
```

Related Commands	Command	Description
	show hosts	Displays the host name buffer table.

Platform N/A

Description

6.2 ip domain-lookup

Use this command to enable DNS domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

ip domain-lookup

no ip domain-lookup

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults This function is enabled by default.

Command Mode Global configuration mode.

Usage Guide This command enables the domain name resolution function.

Configuration Examples The following example disables the DNS domain name resolution function.

```
Ruijie(config)# no ip domain-lookup
```

Related Commands	Command	Description
	show hosts	Displays the DNS related configuration information.

Platform N/A

Description

6.3 ip host

Use this command to configure the mapping of the host name and the IP address. Use the **no** form of the command to remove the host list.

ip host *host-name ip-address*

no ip host *host-name ip-address*

Parameter Description	Parameter	Description
	<i>host-name</i>	The host name of the equipment
	<i>ip-address</i>	The IP address of the equipment

Defaults N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures IPv4 address 192.168.5.243 for domain name www.test.com.

```
Ruijie(config)# ip host www.test.com 192.168.5.243
```

Related	Command	Description
---------	---------	-------------

Commands	
show hosts	Show the DNS related configuration information.

Platform N/A

Description

6.4 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server [**oob**] { *ip-address* | *ipv6-address* } [**via** *mgmt-name*]

no ip name-server [**oob**] [*ip-address* | *ipv6-address*] [**via** *mgmt-name*]

Parameter Description	Parameter	Description
	oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
	<i>ip-address</i>	The IP address of the domain name server.
	<i>ipv6-address</i>	The IPv6 address of the domain name server.
	via	Configures MGMT port.
	<i>mgmt-name</i>	Specifies the MGMT port in oob mode.

Defaults No domain name server is configured by default.

Command Mode Global configuration mode.

Usage Guide Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response.
Up to 6 DNS servers are supported. You can delete a DNS server with the *ip-address* option or all the DNS servers.

Configuration Examples The following example configures the IPv4 domain name server and IPv6 domain name server.

```
Ruijie(config)# ip name-server 192.168.5.134 via mgmt 2/0
Ruijie(config)# ip name-server 2001:0DB8::250:8bff:fee8:f800
2001:0DB8:0:f004::1 via mgmt 2/0
```

Related Commands	Command	Description
	show hosts	Displays the DNS related configuration

	information.
--	--------------

Platform N/A

Description

6.5 ipv6 host

Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the **no** form of the command to remove the host list.

ipv6 host *host-name ipv6-address*

no ipv6 host *host-name ipv6-address*

Parameter Description	Parameter	Description
	<i>host-name</i>	The host name of the equipment
	<i>ipv6-address</i>	The IPv6 address of the equipment

Defaults N/A

Command Global configuration mode.

Mode

Usage Guide To delete the host list, use the **no ipv6 host** *host-name ipv6-address* command.

Configuration The following example configures the IPv6 address for the domain name.

Examples Ruijie(config)# `ipv6 host switch 2001:0DB8:700:20:1::12`

Related Commands	Command	Description
	show hosts	Displays the DNS related configuration information.

Platform N/A

Description

6.6 show hosts

Use this command to display DNS configuration.

show hosts [*hostname*]

Parameter Description	Parameter	Description
	<i>hostname</i>	Displays the specified domain name information,

Defaults All domain name information is displayed by default.

Command Mode Privileged EXEC mode.

Usage Guide This command is used to display the DNS related configuration information.

Configuration Ruijie# show hosts

Examples Name servers are:
192.168.5.134 static

Host	type	Address	TTL(sec)
switch	static	192.168.5.243	---
www.ruijie.com	dynamic	192.168.5.123	126

Field	Description
Name servers	Domain name server
Host	Domain name
type	Resolution type: Static resolution and dynamic resolution.
Address	IP address corresponding to the domain name
TTL	TTL of entries corresponding to the domain name/IP address.

Related Commands

Command	Description
ip host	Configures the host name and IP address mapping by manual.
ipv6 host	Configures the host name and IPv6 address mapping by manual.
ip name-server	Configures the DNS server.

Platform Description N/A

7 FTP Server Commands

7.1 ftp-server enable

Use this command to enable the FTP server. Use the **default** form of this command to restore the default setting.


ftp-server enable
default ftp-server enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the FTP server to connect the FTP client to upload/download the files.

 To enable the FTP client to access to the FTP server files, this command shall be co-used with the **ftp-server topdir** command.

Configuration Examples The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory:

```
Ruijie(config)# ftp-server topdir /syslog
```

The following example disables the FTP Server:

```
Ruijie(config)# no ftp-server enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.2 ftp-server login timeout

Use this command to set the timeout interval for login to the FTP server. Use the **no** or **default** form of this command to restore the default setting.

ftp-server login timeout *time*

no ftp-server login timeout

default ftp-server login timeout

Parameter Description	Parameter	Description
	<i>time</i>	Sets the timeout interval for login to the FTP server, in the range from 1 to 30 in the unit of minutes.

Defaults The default is 2 minutes.

Command Mode Global configuration mode

Usage Guide The timeout interval refers to the maximum time when your account is allowed online after you login to the server. If you don't perform authentication again before the timeout interval expires, you will be forced offline.

Configuration Examples The following example sets the timeout interval for login to the FTP server to 5 minutes.

```
Ruijie(config)# ftp-server login timeout 5
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server login timeout
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.3 ftp-server login times

Use this command to set the number of login attempts. Use the **no** or **default** form of this command to restore the default setting.

ftp-server login times *time*

no ftp-server login times

default ftp-server timeout

Parameter Description	Parameter	Description
	<i>time</i>	Sets the number of login attempts, in the range from 1 to 10.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide The number of login attempts refers to the maximum count you are allowed to perform authentication. If the number of your login attempts exceeds 3, you will be forced offline.

Configuration Examples The following example sets the number of login attempts to 5.

```
Ruijie(config)# ftp-server login times 5
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server login times
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.4 ftp-server timeout

Use this command to set the FTP session idle timeout. Use the **no** or **default** form of this command to restore the default setting.

ftp-server timeout *time*

no ftp-server timeout

default ftp-server timeout

Parameter Description	Parameter	Description
	<i>time</i>	Sets the session idle timeout, in the range from 1 to 3600 in the unit of minutes.

Defaults The default is 10 minutes.

Command Mode Global configuration mode.

Usage Guide Use this command to set the FTP session idle timeout. If the session is idle, the FTP server deems the session connection is invalid and disconnects with the user.

 The session idle time refers to the time for the FTP session between two FTP operations

Configuration The following example sets the session idle timeout to 5 minutes:

Examples

```
Ruijie(config)# ftp-server timeout 5
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server timeout
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

7.5 ftp-server topdir

Use this command to set the directory range for the FTP client to access to the FTP server files. Use the **no** or **default** form of this command to restore the default setting.

ftp-server topdir *directory*

no ftp-server topdir

default ftp-server topdir

Parameter Description

Parameter	Description
<i>directory</i>	Sets the top-directory.

Defaults No top-directory is configured by default.

Command Mode Global configuration mode.

Usage Guide The FTP server top directory specifies the directory range of the files accessed by the client. Can the FTP client accesses to the files on the FTP server with the top directory correctly specified. Without this command configured, FTP client fails to access to any file or directory on the FTP server.

Configuration The following example enables the FTP Server and confines the FTP client access to the syslog

Examples subdirectory.

```
Ruijie(config)# ftp-server topdir /syslog
Ruijie(config)# ftp-server enable
```

The following example restores the default setting.

```
Ruijie(config)# no ftp-server topdir
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

7.6 ftp-server username password

Use this command to set the login username and password for the FTP server. Use the **no** form of this command to restore the default setting.

ftp-server username *username* **password** [*type*] *password*

no ftp-server username *username*

default ftp-server username *username*

**Parameter
Description**

Parameter	Description
<i>username</i>	Sets the login username.
<i>password</i>	Sets the log password

Defaults No username or password is set by default.

**Command
Mode** Global configuration mode

Usage Guide Use this command to set the login username for the FTP server. To log in to the FTP server, the correct username and password shall be provided.

The maximum length of the username is 64 characters and the spaces are not allowed in the middle of the username. The username consists of letters, semiangle number and semiangle mark. One username can be configured for the FTP server at most.

The password must contain letters or numbers. Spaces before or behind the password are allowed but will be ignored. The spaces within are part of the password.

The plaintext password is in the range from 1 to 25 characters. The encrypted password is in the range from 4 to 52 characters.

 The anonymous user login is not supported on the FTP server. The client fails to pass the

identity verification if the username is removed.

Configuration The following example sets the username to user:

Examples

```
Ruijie(config)# ftp-server username user password pass
```

The following example restores the default setting:

```
Ruijie(config)# no ftp-server username user
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.7 show ftp-server

Use this command to show the status information of the FTP server.

show ftp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The FTP server status information includes:

- Enabled/Disabled server
- The FTP server top directory
- The FTP server user information, including username, password and connection number. If connection is set up, the IP address, port, transmission type, active/passive mode is shown

Configuration Examples The following example displays the related status information of the FTP server:

```
Ruijie#show ftp-server
ftp-server information
```

```

=====
enable : Y
topdir : tmp:/
timeout: 10min
username:aaaa      password:(PLAIN)bbbb      connect num[2]
[0]trans-type:BINARy (ctrl)server IP:192.168.21.100[21]
client IP:192.168.21.26[3927]
[1]trans-type:ASCIIf (ctrl)server IP:192.168.21.100[21]
client IP:192.168.21.26[3929]
username:a1        password:(PLAIN)bbbb      connect num[0]
username:a2        password:(PLAIN)bbbb      connect num[0]
username:a3        password:(PLAIN)bbbb      connect num[0]
username:a4        password:(PLAIN)bbbb      connect num[0]
username:a5        password:(PLAIN)bbbb      connect num[0]
username:a6        password:(PLAIN)bbbb      connect num[0]
username:a7        password:(PLAIN)bbbb      connect num[0]
username:a8        password:(PLAIN)bbbb      connect num[0]
username:a9        password:(PLAIN)bbbb      connect num[0]
    
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8 FTP Client Commands

8.1 copy flash

Use this command to upload the file from the server to the device through FTP Client.

copy flash: *[local-directory/] local-file ftp://username:password@dest-address [/remote-directory] /remote-file*

Parameter Description	Parameter	Description
	<i>username</i>	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	<i>password</i>	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	<i>dest-address</i>	IP address of the target FTP Server.
	<i>remote-directory</i>	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
	<i>remote-file</i>	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
	<i>local-directory</i>	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
	<i>local-file</i>	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example uploads the file named "local-file" in directory "home" of local device to directory "root" on the FTP Server whose user name is user, password is pass and IP address is 192.168.23.69, and changes the filename to "remote-file".

Examples

```
Ruijie# copy flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

8.2 copy ftp

Use this command to download the file from the server to the device through FTP Client.

```
copy ftp://username:password@dest-address [ /remote-directory ] / remote-file
flash:[ local-directory/ ] local-file]
```

Parameter Description

Parameter	Description
<i>username</i>	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
<i>password</i>	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
<i>dest-address</i>	IP address of the target FTP Server.
<i>remote-directory</i>	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
<i>remote-file</i>	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
<i>local-directory</i>	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
<i>local-file</i>	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example uses username of "user" and password of "pass" to download a file named "remote-file" from the directory "root" on FTP Server with IP address 192.168.23.69 to directory "home" on the local device, and changes the name to "local-file".

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file
flash:home/local-file
```

Related Commands

Command	Description
copy tftp	Uses the TFTP protocol to transfer files.

Platform Description N/A

8.3 ftp-client ascii

Use this command to use ASCII mode for FTP transfer.

Use the **no** form of this command to restore the default setting.

ftp-client [vrf vrfname] ascii

no ftp-client [vrf vrfname] ascii

default ftp-client [vrf vrf-name]

Parameter Description

Parameter	Description
vrf vrf-name	Configures the file transfer mode for the specified VRF.

Defaults The default FTP transfer mode is binary.

Command Mode Global configuration mode

Usage Guide The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

Configuration Examples The following example configures ASCII FTP transfer.

```
Ruijie (config)# ftp-client ascii
```

The following example configures ASCII FTP transfer for *vrf-name*.

```
Ruijie(config)# ftp-client vrf vrf-name ascii
```

The following example configures binary FTP transfer.

```
Ruijie(config)# no ftp-client ascii
```

The following example configures binary FTP transfer for *vrf-name*.

```
Ruijie(config)# no ftp-client vrf vrf-name ascii
```

The following example restores the default setting of the FTP Client.

```
Ruijie(config)# default ftp-client
```

The following example restores the default setting of the FTP Client *vrf-name*,

```
Ruijie(config)# default ftp-client vrf vrf-name
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

8.4 ftp-client port

Use this command to configure PORT mode used for FTP data connection. Use the **no** form of this command to restore the default setting.

ftp-client [vrf *vrfname*] port

no ftp-client [vrf *vrfname*] port

default ftp-client [vrf *vrf-name*]

Parameter Description

Parameter	Description
vrf <i>vrf-name</i>	VRF name The default is the public network instance.

Defaults The default is PASV mode for FTP data connection.

Command Mode Global configuration mode.

Usage Guide This command is used to configure the connection mode to PORT mode, in which the server will actively connect with the client.

The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

Configuration Examples The following example configures PORT mode used for FTP data connection

```
Ruijie (config)# ftp-client port
```

The following example configures PORT mode used for FTP *vrf-name* data connection.

```
Ruijie(config)# ftp-client vrf vrf-name port
```

The following example configures PASV mode for FTP data connection.

```
Ruijie(config)# no ftp-client port
```

The following example configures PASV mode used for FTP *vrf-name* data connection.

```
Ruijie(config)# no ftp-client vrf vrf-name port
```

The following example restores the default setting of the FTP Client.

```
Ruijie(config)# default ftp-client
```

The following example restores the default setting of the FTP Client *vrf-name*,

```
Ruijie(config)# default ftp-client vrf vrf-name
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

8.5 ftp-client source

Use this command to bind FTP Client with the source IP address of client and use this IP address to communicate with server. Use the **no** form of this command to disable source IP address binding. Use the **default** form of this command to restore the default setting.

ftp-client [vrf vrf-name] source { ip-address | ipv6-address | interface }

no ftp-client [vrf vrf-name] source

default ftp-client [vrf vrf-name]

Parameter Description	Parameter	Description
	vrf vrf-name	

Defaults By default, the IP address is not bound with the client locally. Instead, it is selected by the route.

Command Mode Global configuration mode

Usage Guide The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound. The **ftp-client [vrf vrfname] source-address { ip-address | ipv6-address }** command will be converted to this command automatically

Configuration Examples The following example binds FTP Client with source IP address 192.168.23.236.

```
Ruijie(config)# ftp-client source 192.168.23.236
```

The following example binds FTP Client with source IP address 2003:0:0:0::2.

```
Ruijie(config)# ftp-client source 2003:0:0:0::2
```

The following example binds FTP Client *vrf-name* with source IP address 192.168.23.236.


```
Ruijie(config)# ftp-client vrf vrf-name source 192.168.23.236
```

The following example binds FTP Client *vrf-name* with source IP address 2003:0:0:0::2.

```
Ruijie(config)# ftp-client vrf vrf-name source 2003:0:0:0::2
```

The following example disables source IP address binding.

```
Ruijie(config)# no ftp-client source
```

The following example disables source IP address binding.

```
Ruijie(config)# no ftp-client vrf vrf-name source
```

The following example restores the default setting of the FTP Client.

```
Ruijie(config)# default ftp-client
```

The following example restores the default setting of the FTP Client vrf-name,

```
Ruijie(config)# default ftp-client vrf vrf-name
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

9 Tunnel Commands

9.1 show interfaces tunnel

Use this command to display the tunnel configuration.

show interfaces tunnel [*number*]

Parameter Description	Parameter	Description
	<i>number</i>	Specifies the tunnel number.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays tunnel 1 information.

```
Ruijie#showinterfaces tunnel 1
// Here is the public information about the interface
Tunnel source 1.1.1.2, destination 1.1.1.1, routeable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport is ipv6ip
  Tunnel transport VPN is no set
```

Field Description

Field	Description
Destination	The tunnel destination address. The address 0.0.0.0 indicates that the destination address is not configured.
Tunnel source	The tunnel source address, which can be either an IPv4 or an IPv6 address. If the tunnel source interface command is configured, the tunnel source address is the interface address.
Tunnel TTL	The TTL or hop limit field of the transmission protocol.
Tunnel TOS	The TOS or traffic class field of the transmission protocol. Note that there is an exception. If the field is 0, and the transmission protocol is the same as the payload protocol, the field of the payload protocol is copied to the

	transmission protocol.
Tunnel nested-limit	The limit to the number of tunnel nested encapsulation times. This field is displayed by all tunnels except the 6to4, 6rd and isatap tunnels.
Tunnel protocol/transport	Tunnel encapsulation mode
Key	With the key setting, this field is displayed by only the GRE tunnel.
Checksuming	With the checksum setting, this field is displayed by only the GRE tunnel.
Tunnel VPN	The destination VRF.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.2 show tunnel statistics

Use this command to display the number of configurable tunnel interfaces and configured tunnel interfaces.

show tunnel statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display the number of configurable tunnel interfaces and configured tunnel interfaces. Note that the actual forwarding capacity is restricted by the number of chipentries. It is possible that the tunnel interface has been created while the chip entry list is full. In that case, the syslog is generated.

Configuration Examples

The following example displays the number of configurable tunnel interfaces and configured tunnel interfaces.

```
Ruijie#show tunnel statistics
used: 2, limit: 1000
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.3 tunnel destination

Use this command to specify the destination IP address of a tunnel interface in interface configuration mode.

Use the **no** form of this command to restore the default setting.

tunnel destination *ip-address*

no tunnel destination

Parameter Description	Parameter	Description
	<i>ip-address</i>	Sets the IP address of the specified tunnel destination.

Defaults No destination IP address is set by default.

Command Mode Interface configuration mode

Usage Guide This command must be used to specify the peer address during tunnel setup. Tunnels cannot be set up if this command is not executed.

Configuration Examples The following example creates a tunnel interface.

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if)# tunnel mode gre ip
```

The following example sets the destination IP address of tunnel interface.

```
Ruijie(config-if)# tunnel destination 1.1.1.1
```

Related Commands	Command	Description
	show interface tunnel	Displays tunnel interface information.

Platform Description N/A

9.4 tunnel mode

Use this command to set the encapsulation mode on a tunnel interface.

Use the **no** or **default** form of this command to restore to the default setting.

tunnel mode { gre {ip | ipv6} | ipv6 | ipip | ipv6ip [6to4 | isatap] }

no tunnel mode

default tunnel mode

Parameter Description	Parameter	Description
	gre ip	The transmission network is IPv4 network. GRE for the route is at the IP layer
	gre ipv6	The transmission network is IPv6 network. GRE for the route is at the IP layer
	ipv6	The transmission network is IPv6 network. GRE for the route is not at the IP layer.
	ipip	The transmission network is IPv4 network. GRE for the route is not at the IP layer. The user network is IPv4 network.
	ipv6ip	The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is manually configured IPv6 network. The IPv4 address of the peer end needs to be configured.
	ipv6ip 6to4	The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is IPv6 network. The IPv4 address of the peer end does not need to be configured. It is used for connection between IPv6 networks.
	ipv6ip isatap	The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is IPv6 network. The IPv4 address of the peer end does not need to be configured. It is used for quick deployment of IPv6 networks.

Defaults For switches and wireless products, the default encapsulation mode is **ipv6ip**.
For gateways and routers, the default encapsulation mode is **gre ip**.

Command Mode Interface configuration mode

Usage Guide The tunnel encapsulation format is the tunnel carrier protocol. The default encapsulation format of tunnel interfaces is GRE. You can determine the encapsulation format of tunnel interfaces based on the actual usage. By default, IP tunnel GRE can be implemented without any definition of the encapsulation format.

Configuration The following example creates a tunnel interface.

Examples

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

**Related
Commands**

Command	Description
show interface tunnel	Displays tunnel interface information.

**Platform
Description**

N/A

9.5 tunnel source

Use this command to configure the source IP address for the tunnel.

Use the no form of this command to restore the default setting.

tunnel source { *ip-address* | *interface-type interface-number* }

no tunnel source

**Parameter
Description**

Parameter	Description
<i>ip-address</i>	Source IP address of the tunnel used as the source IP address of the packets to be transmitted through the tunnel.
<i>interface-type</i> <i>interface-number</i>	Interface referenced by the tunnel, which will be used as the source IP address of the packets to be transmitted through the tunnel.

Defaults No tunnel source address is configured by default.

Command Interface configuration mode.

Mode

Usage Guide The source IP address of a tunnel can be a specified IP address or an IP address of an interface. When you configure an auto tunnel (for example, 6to4 and isatap), it is recommended to specify the source address.

A device shall not be configured multiple tunnels with the same encapsulation type, source address and destination address.

If there are multiple auto tunnels, their source addresses shall be different.

Configuration The following example creates a tunnel interface.

Examples

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

The following example configures an IPv6 manual tunnel.

```
Ruijie(config-if)# tunnel source 1.1.1.1
```

Related Commands	Command	Description
	tunnel mode	Configures the mode of a tunnel.
	tunnel destination	Configures the destination address of a tunnel.
	Tunnel ttl	Configures the TTL of the tunnel.

Platform N/A

Description

9.6 tunnel tos

Use this command to set the IPv4 ToS byte or IPv6 traffic class 8 bits in tunnel interface configuration mode. Use the **no** form of this command to restore the default setting.

tunnel tos *number*

no tunnel tos

Parameter Description	Parameter	Description
	<i>number</i>	IPv4 ToS byte or IPv6 traffic class 8 bits, in the range from 0 to 255.

Defaults By default, the inner-layer IPv4 ToS byte is copied to the outer-layer IPv4 header, if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the IPv4 protocol. By default, the inner-layer IPv6 traffic class 8 bits are copied to the outer-layer IPv6 header if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the Ipv6 protocol. In other circumstances, the outer-layer IPv4 ToS and IPv6 traffic class are 0.

Command

Mode Interface configuration mode

Usage Guide This command is used to set GRE tunnel packets to a higher priority.

Configuration Examples The following example sets the ToS byte for a GRE tunnel outer-layer encapsulation protocol to 100 on interface tunnel 1.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel mode ipv6ip
Ruijie(config-if)# tunnel tos 100
```

Related Commands	Command	Description
	show interface tunnel	Displays tunnel interface information.

Platform N/A

Description

9.7 tunnel ttl

Use this command to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages.

Use the **no** form of this command to restore the default setting.

tunnel ttl *hop-count*

no tunnel ttl

Parameter	Parameter	Description
Description	<i>hop-count</i>	TTL value

Defaults The default is 255.

Command Interface configuration mode

Mode

Usage Guide This command is used to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages.

Configuration The following example creates a tunnel interface.

Examples

```
Ruijie(config)# interface tunnel 1
```

The following example configures the tunnel mode.

```
Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip
```

The following example sets the TTL value to 100.

```
Ruijie(config-if)# tunnel ttl 100
```

Related Commands	Command	Description
	tunnel mode	Configures the mode of a tunnel.
	tunnel source	Configures the source IP address of the tunnel.
	tunnel destination	Configures the destination IP address of a tunnel.

Platform N/A

Description

10 Network Connectivity Test Tool Commands

10.1 clear rping table all

Use this command to clear Rping entries.

clear rping table [**all** | [**ping-object** *owner test-name*] | [**trace-object** *owner test-name*]]

Parameter Description	Parameter	Description
	<i>owner</i>	User index
	<i>test-name</i>	Test index

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all Rping entries.

```
Ruijie# clear rping table all
```

The following example clears the specified Rping entry.

```
Ruijie# clear rping table user ruijie
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.2 ping

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

ping [**oob** | **vrf** *vrf-name* | **ip**] [**address** [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** *millisecond*] [**out-interface** *interface*] [**next-hop** *next-hop*]]

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

n

oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
<i>vrf-name</i>	VRF name
<i>address</i>	Specifies an IPv4 address.
<i>mgmt-name</i>	Specifies the MGMT port in OOB mode.
<i>length</i>	Specifies the length of the packet to be sent (range: 36-18024, default: 100).
<i>times</i>	Specifies the number of packets to be sent (range:1- 4294967295).
<i>seconds</i>	Specifies the timeout time (range: 1-10 seconds).
<i>data</i>	Specifies the data to fill in.
<i>source</i>	Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address.
df-bit	Sets the DF bit for the IP address. DF bit=1 indicates not to segment the datagrams. By default, the DF bit is 0.
validate	Sets whether to validate the reply packets or not.
detail	Sets whether to contain details in the echoed message. By default, only “!” and “.” are displayed.
<i>interface</i>	Specifies the outbound interface
<i>next-hop</i>	Specifies the next hop IPv4 address
<i>millisecond</i>	Specifies the ping interval, in the range from 10 to 300000 milliseconds. Default: 100 milliseconds.

Defaults Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

Command Privileged EXEC mode.

Mode

Usage If the device can be pinged, the response information is displayed, and the statistics is listed at the end. For

Guide the extension functions of ping, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Configurat The following example tests the connectivity of a network to locate the network connectivity problem.

```
(regular ping).Ruijie# ping 192.168.21.26
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
 < press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example displays details.

```
Ruijie#ping 192.168.21.26 detail
*Apr 16 09:16:08: %PING-7-DEBUG: Ping vrf index -1.
```

```
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
 < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.2
```

The following example tests the connectivity of a network to locate the network connectivity problem (extension ping).

```
Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99
timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
 < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

The following example displays the details.

```
ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3
detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
 < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
```

```
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms
```

Related Command s	Command	Description
	N/A	N/A

Platform N/A

Description
n

10.3 ping ipv6

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

```
ping [ vrf vrf-name | [ oob ] ipv6 ] [ ip-address [ via mgmt-name ] [ length length ] [ ntimes times ] [ timeout seconds ] [ data data ] [ source source ] [ detail ] [ interval millisecond ] [ out-interface interface [ next-hop next-hop ] ]
```

Parameter Description n	Parameter	Description
	oob	
<i>vrf-name</i>		VRF name
<i>ip-address</i>		Specifies an IPv6 address.
<i>mgmt-name</i>		Specifies the MGMT port in OOB mode.
<i>length</i>		Specifies the length of the packet to be sent (range: 36-18024, default: 100).
<i>times</i>		Specifies the number of packets to be sent (range:1-4294967295).
<i>seconds</i>		Specifies the timeout time (range: 1-10 seconds).
<i>data</i>		Specifies the data to fill in.
<i>source</i>		Specifies the source IPv6 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address.
detail		Sets whether to contain details in the echoed message. By default, only “!” and “.” are displayed.
<i>interface</i>		Specifies the outbound interface
<i>next-hop</i>		Specifies the next hop IPv6 address
<i>millisecond</i>		Specifies the ping interval, in the range from 10 to 300000 milliseconds. Default: 100 milliseconds.

Defaults Five packets with 100Byte in length are sent to the specified IP address within specified time 2 seconds by default

Command Privileged EXEC mode.

Mode

Usage If the device can be pinged, the response information is displayed, and the statistics is listed at the end. If the

Guide response data does not match the request data, a 'Request receive error.' message is displayed and the statistics is listed in the end. For the extension functions of ping ipv6, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Configurat The following example tests the connectivity of a network to locate the network connectivity problem.

ion

Examples

```
(regular ping) Ruijie# ping ipv6 2001::5
Sending 5, 100-byte ICMP Echoes to 2001::5, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example displays details.

```
Ruijie#ping 2001::1 detail
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
< press Ctrl+C to break >
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

The following example tests the connectivity of a network to locate the network connectivity problem (extension ping).

```
Ruijie# ping ipv6 2001::5 length 1500 ntimes 100 data ffff source 2001::9 timeout 3
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds:
< press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

The following example displays the details.

```
Ruijie#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3
Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds:
< press Ctrl+C to break >
Reply from 2001::5: bytes=1500 time=1ms
```

```
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
```

**Related
Command
s**

Command	Description
N/A	N/A

Platform N/A

Description

10.4 show rping detail

Use this command to display Rping information.

show rping detail

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display the Rping information such as numbers of test accounts and users.

Configuration Examples The following example displays Rping information.

```
Ruijie#show rping detail
Total owner number: 2
Total test number: 4
owner: user1
  test name: taget_1      storage type: volatile
test name: taget_2      storage type: nonVolatile
```

```
owner: user2
  test name: taget_1      storage type: permanent
test name: taget_2      storage type: readOnly
```

Field	Description
Total owner number	The number of users
Total test number	The number of Rping accounts
owner	Username
test name	Test name
storage type	Storage type

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

10.5 traceroute

Use this command to display all gateways passed by the test packets from the source address to the destination address.

traceroute [**oob** | **vrf** *vrf-name* | **ip**] [*address* [**via** *mgmt-name*]] [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** *interface* [**next-hop** *next-hop*]]

Parameter Description	Parameter	Description
	oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
	<i>vrf-name</i>	VRF name
	<i>address</i>	Specifies an IPv4 address.
	<i>mgmt-name</i>	Specifies the MGMT port in OOB mode.
	<i>number</i>	Specifies the number of probe packets to be sent (range: 1-255).
	<i>source</i>	Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address.
	<i>seconds</i>	Specifies the timeout time (range: 1-10 seconds).
	<i>minimum maximum</i>	Specifies the minimum and maximum TTL values (range:1-255).
	<i>interface</i>	Specifies the outbound interface
	<i>next-hop</i>	Specifies the next hop IPv4 address

Defaults By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

Command Privileged EXEC mode: enables extended functions.

Mode User EXEC mode: enables basic functions.

Usage Guide Use the **traceroute** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

Configuration Examples The following is two examples of the application about traceroute, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
Ruijie# traceroute 61.154.22.36
< press Ctrl+C to break >
Tracing the route to 61.154.22.36

 1  192.168.12.1      0 msec  0 msec  0 msec
 2  192.168.9.2       4 msec  4 msec  4 msec
 3  192.168.9.1       8 msec  8 msec  4 msec
 4  192.168.0.10      4 msec  28 msec 12 msec
 5  192.168.9.2       4 msec  4 msec  4 msec
 6  202.101.143.154   12 msec  8 msec  24 msec
 7  61.154.22.36     12 msec  8 msec  22 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42

 1  192.168.12.1      0 msec  0 msec  0 msec
 2  192.168.9.2       0 msec  4 msec  4 msec
 3  192.168.110.1     16 msec 12 msec 16 msec
 4  * * *
 5  61.154.8.129      12 msec 28 msec 12 msec
 6  61.154.8.17       8 msec 12 msec 16 msec
 7  61.154.8.250      12 msec 12 msec 12 msec
 8  218.85.157.222    12 msec 12 msec 12 msec
 9  218.85.157.130    16 msec 16 msec 16 msec
10  218.85.157.77     16 msec 48 msec 16 msec
11  202.97.40.65      76 msec 24 msec 24 msec
12  202.97.37.65      32 msec 24 msec 24 msec
13  202.97.38.162     52 msec 52 msec 224 msec
14  202.96.12.38      84 msec 52 msec 52 msec
15  202.106.192.226   88 msec 52 msec 52 msec
16  202.106.192.174   52 msec 52 msec 88 msec
```



```

17      210.74.176.158  100 msec  52 msec  84 msec
18      202.108.37.42   48 msec   48 msec  52 msec

```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent time are displayed, and gateway 4 fails.

```

Ruijie# traceroute www.ietf.org

Translating "www.ietf.org"...[OK]
  < press Ctrl+C to break >
Tracing the route to 64.170.98.32

 1      192.168.217.1      0 msec  0 msec  0 msec
 2      10.10.25.1         0 msec  0 msec  0 msec
 3      10.10.24.1        0 msec  0 msec  0 msec
 4      10.10.30.1       10 msec  0 msec  0 msec
 5      218.5.3.254      0 msec  0 msec  0 msec
 6      61.154.8.49     10 msec  0 msec  0 msec
 7      202.109.204.210  0 msec  0 msec  0 msec
 8      202.97.41.69    20 msec  10 msec  20 msec
 9      202.97.34.65    40 msec  40 msec  50 msec
10     202.97.57.222    50 msec  40 msec  40 msec
11     219.141.130.122  40 msec  50 msec  40 msec
12     219.142.11.10   40 msec  50 msec  30 msec
13     211.157.37.14   50 msec  40 msec  50 msec
14     222.35.65.1     40 msec  50 msec  40 msec
15     222.35.65.18    40 msec  40 msec  40 msec
16     222.35.15.109   50 msec  50 msec  50 msec
17     *      *      *
18     64.170.98.32    40 msec  40 msec  40 msec

```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

10.6 traceroute ipv6

Use this command to display all gateways passed by the test packets from the source address to the destination address.

```

traceroute [ vrf vrf-name | [ oob ] ipv6 ] [ address [ via mgmt-name ] [ probe number ] [ timeout
seconds ] [ tll minimum maximum ] [ out-interface interface [ next-hop next-hop ] ] ]

```

Parameter

Parameter	Description
-----------	-------------

Description	
oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
<i>vrf-name</i>	VRF name
<i>address</i>	Specifies an IPv6 address.
<i>mgmt-name</i>	Specifies the MGMT port in OOB mode.
<i>number</i>	Specifies the number of probe packets to be sent.
<i>seconds</i>	Specifies the timeout time.
<i>minimum maximum</i>	Specifies the minimum and maximum TTL values.
<i>interface</i>	Specifies the outbound interface
<i>next-hop</i>	Specifies the next hop IPv6 address

Defaults By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

Command Privileged EXEC mode: enables extended functions.

Mode User EXEC mode: enables basic functions.

Usage Guide Use the **traceroute ipv6** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

Configuration Examples The following is two examples of the application about traceroute ipv6, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
Ruijie# traceroute ipv6 3004::1
< press Ctrl+C to break >
Tracing the route to 3004::1
 1  3000::1      0 msec  0 msec  0 msec
 2  3001::1      4 msec  4 msec  4 msec
 3  3002::1      8 msec  8 msec  4 msec
 4  3004::1      4 msec  28 msec 12 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~4) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute ipv6 3004::1
< press Ctrl+C to break >
Tracing the route to 3004::1
 1  3000::1      0 msec  0 msec  0 msec
 2  3001::1      4 msec  4 msec  4 msec
 3  3002::1      8 msec  8 msec  4 msec
 4  * * *
 5  3004::1      4 msec  28 msec 12 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP

address of 3004::1 (gateways 1~5) and the spent time are displayed, and gateway 4 fails.

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

11 TCP Commands

11.1 ip tcp keepalive

Use this command to enable the TCP keepalive function. Use the **no** form of this command to restore the default setting,

ip tcp keepalive [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]

Parameter Description

Parameter	Description
interval <i>num1</i>	The interval of sending the keepalive packet, in the range from 1 to 120 in the unit of seconds, The default is 75.
times <i>num2</i>	Keepalive packet sending times, in the range from 1 to 10. The default is 6.
idle-period <i>num3</i>	Idle time, the time period during which the peer end does not send any packet to the local end, in the range from 60 to 1,800 in the unit of seconds. The default is 900.

Defaults The function is disabled by default.

Command Mode Global configuration mode

Usage Guide The keepalive function enables TCP to detect whether the peer end is operating properly. Suppose the keepalive function is enabled together with default **interval**, **times** and **idle-period** settings. TCP begins to send the keepalive packet at an interval of 75 seconds if it does not receive any packet from the peer end in 900 seconds. The TCP connection is considered invalid and then disconnected automatically if the device sends the keepalive packet for six consecutive times without receiving any TCP packet from the peer end. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example enables the TCP keepalive function on the device and sets the **idle-period** and **interval** to 180 and 60 respectively. If the device sends the keepalive packet for four consecutive times without receiving any TCP packet from the peer end, the TCP connection is considered invalid.

```
Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

Related Commands

Command	Description
N/A	N/A

Platform Description

11.2 ip tcp mss

Use this command to set the upper limit of the MSS value. Use the **no** form of this command to restore the default setting.

ip tcp mss *max-segment-size*

no ip tcp mss

Parameter Description	Parameter	Description
	<i>max-segment-size</i>	Upper limit of the MSS value in the range from 68 to 10,000 bytes

Defaults The default MSS = Outgoing IPv4/v6 MTU- IPv4/v6 header-TCP header.

Command Mode Global configuration mode

Usage Guide This command is used to limit the maximum value of MSS for the TCP connection to be created. The negotiated MSS cannot exceed the configured value. You can use this command to reduce the maximum value of MSS. However, this configuration is not needed in general. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example sets the upper limit of the MSS value to 1,300 bytes.

```
Ruijie(config)# ip tcp mss 1300
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

11.3 ip tcp path-mtu-discovery

Use this command to enable Path Maximum Transmission Unit (PMTU) discovery function for TCP in global configuration mode. Use the **no** form of this command to restore the default setting.

ip tcp path-mtu-discovery [**age-timer** *minutes* | **age-timer infinite**]

no ip tcp path-mtu-discovery

Parameter Description	Parameter	Description
	age-timer <i>minutes</i>	The time interval for further discovery after discovering PMTU. Its value ranges from 10 to 30 minutes. The default value is 10.
	age-timer infinite	No further discovery after discovering PMTU

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Based on RFC1191, the TCP path MTU function improves the network bandwidth utilization and data transmission when the user uses TCP to transmit the data in batch. Enabling or disabling this function takes no effect for existent TCP connections and is only effective for TCP connections to be created. This command applies to only IPv4 TCP. This function is enabled for IPv6 TCP constantly and cannot be disabled. According to RFC1191, after discovering the PMTU, the TCP uses a greater MSS to detect the new PMTU at a certain interval, which is specified by the parameter **age-timer**. If the PMTU discovered is smaller than the MSS negotiated between two ends of the TCP connection, the device will be trying to discover the greater PMTU at the specified interval until the PMTU value reaches the MSS or the user stops this timer. Use the parameter **age-timer infinite** to stop this timer.

Configuration The following example enables PMTU discovery.

Examples Ruijie(config)# ip tcp path-mtu-discovery

Related Commands	Command	Description
		show tcp pmtu

Platform Description N/A

11.4 ip tcp send-reset

Use this command to enable the device to send the reset packet when receiving the TCP port unreachable packet. Use the **no** form of this command to disable this function,

ip tcp send-reset
no ip tcp send-reset

Parameter Description	Parameter	Description
		N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide In general, when dispatching the TCP packet, the TCP module replies a reset packet automatically to disconnect the TCP connection with the peer end if the TCP connection that this packet belongs to is not found. However, flooding TCP port unreachable packets pose an attack threat to the device. This command can be used to disable the device from sending the reset packet when receiving the TCP port unreachable packet. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example disables the device from sending the reset packet when receiving the TCP port unreachable packet.

```
Ruijie(config)# no ip tcp send-reset
```

Related Commands

Command	Description
N/A	N/A

Platform Description

11.5 ip tcp synwait-time

Use this command to set the timeout value for SYN packets (the maximum time from SYN transmission to successful three-way handshake). Use the **no** form of this command to restore the default setting.

ip tcp synwait-time *seconds*

no ip tcp synwait-time

Parameter Description

Parameter	Description
<i>seconds</i>	Timeout value for SYN packets in the range from 5 to 300 in the unit of seconds.

Defaults The default is 20.

Command Mode Global configuration mode

Usage Guide If there is an SYN attack in the network, reducing the SYN timeout value can prevent resource consumption, but it takes no effect for successive SYN attacks. When the device actively requests a connection with an external device, reducing the SYN timeout value can shorten the time for the user to wait, such as telnet login. For poor network conditions, the timeout value can be increased properly. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example set the timeout value for SYN packets to 10 seconds.

```
Ruijie(config)# ip tcp syntime-out 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

11.6 ip tcp window-size

Use this command to change the size of receiving buffer and sending buffer for TCP connections. Use the **no** form of this command to restore the default setting.

ip tcp window-size *size*

no ip tcp window-size

Parameter Description	Parameter	Description
	<i>size</i>	

Defaults The default is 65,535 bytes.

Command Mode Global configuration mode

Usage Guide The TCP receiving buffer is used to buffer the data received from the peer end. These data will be subsequently read by application programs. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For connections involving a large bandwidth and mass data, increasing the size of receiving buffer will remarkably improve TCP transmission performance. If the window size is greater than 65535 bytes, window enlarging will be enabled automatically.

Configuration Examples The following example sets the TCP window size to 16,386 bytes.

```
Ruijie(config)# ip tcp window-size 16386
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

11.7 service tcp-keepalives-in

Use this command to enable the keepalive function for the TCP server. Use the no form of this

command to restore the default setting.

service tcp-keepalives-in [*interval*] [**garbage**]

no service tcp-keepalives-in

**Parameter
Description**

Parameter	Description
<i>interval</i>	The interval of sending keepalive packets, in the range from 1 to 65535 in the unit of seconds. The default is 60.
garbage	The keepalive packet contains one-byte invalid data. The invalid data is not contained by default.

Defaults This function is disabled by default.

**Command
Mode** Global configuration mode

Usage Guide The keepalive function enables the TCP server to detect whether the client is operating properly. If the TCP server sends the keepalive packet for four consecutive times without receiving any TCP packet from the client, the TCP connection is considered invalid and then is disconnected automatically.

**Configuration
Examples** The following example enables the keepalive function for the TCP server and sets the interval of sending the keepalive packet to 10 seconds. The keepalive packet contains one-byte invalid data.

```
Ruijie(config)# service tcp-keepalives-in 10 garbage
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** When you run this RGOS 10.x command, it is converted to the **ip tcp keepalive** command automatically in RGOS 11.0.

11.8 service tcp-keepalives-out

Use this command to enable the keepalive function for the TCP client. Use the **no** form of this command to restore the default setting,

service tcp-keepalives-out [*interval*] [**garbage**]

**Parameter
Description**

Parameter	Description
<i>interval</i>	The interval of sending keepalive packets, in the range from 1 to 65535 in the unit of seconds. The default is 60.

garbage	The keepalive packet contains one-byte invalid data. The invalid data is not contained by default.
----------------	--

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The keepalive function enables the TCP client to detect whether the server is operating properly. If the TCP client sends the keepalive packet for four consecutive times without receiving any TCP packet from the server, the TCP connection is considered invalid and then is disconnected automatically.

Configuration Examples The following example enables the keepalive function for the TCP client and sets the interval of sending the keepalive packet to 10 seconds. The keepalive packet contains one-byte invalid data

```
Ruijie(config)# service tcp-keepalives-out 10 garbage
```

Related Commands	Command	Description
	N/A	N/A

Platform Description When you run this RGOS 10.x command, it is converted to the **ip tcp keepalive** command automatically in RGOS 11.0.

11.9 show ipv6 tcp connect

Use this command to display the current IPv6 TCP connection information.

```
show ipv6 tcp connect [ local-ipv6 X:X:X:X::X ] [ local-port num ] [ peer-ipv6 X:X:X:X::X ] [ peer-port num ]
```

Use this command to display the current IPv6 TCP connection statistics.

```
show ipv6 tcp connect statistics
```

Parameter Description	Parameter	Description
	local-ipv6 X:X:X:X::X	
local-port <i>num</i>		Local port
peer-ipv6 X:X:X:X::X		Peer IPv6 address
peer-port <i>num</i>		Peer port
statistics		Displays IPv6 TCP connection statistics

Defaults N/A

Command Privileged EXEC mode
Mode

Usage Guide N/A

Configuration The following example displays the current IPv6 TCP connection information.

```

Examples Ruijie#show ipv6 tcp connect
Number Local Address      Foreign Address          State      Process name
1      :::22                   :::0                     LISTEN    rg-sshd
2      :::23                   :::0                     LISTEN    rg-telnetd
3      1000::1:23            1000::2:64201          ESTABLISHED  rg-telnetd

The following example displays the current IPv6 TCP connection statistics.
Ruijie#show ipv6 tcp connect statistics
State      Count
-----
ESTABLISHED 1
SYN_SENT   0
SYN_RECV   0
FIN_WAIT1  0
FIN_WAIT2  0
TIME_WAIT  0
CLOSED     0
CLOSE_WAIT 0
LAST_ACK   0
LISTEN     1
CLOSING    0
Total: 2
    
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

11.10 show ipv6 tcp pmtu

Use this command to display information about IPv6 TCP PMTU.

show ipv6 tcp pmtu [local-ipv6 X:X:X:X::X] [local-port num] [peer-ipv6 X:X:X:X::X] [peer-port num]

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

local-ipv6 <i>X:X:X:X::X</i>	Local IPv6 address
local-port <i>num</i>	Local port
peer-ipv6 <i>X:X:X:X::X</i>	Peer IPv6 address
peer-port <i>num</i>	Peer port

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example information about IPv6 TCP PMTU.

Examples

```
Ruijie# show ipv6 tcp pmtu
Number  Local Address          Foreign Address          PMTU
1       1000::1:23             1000::2.13560
```

Field	Description
Number	Number
Local Address	Local address and port number. The number after the last colon is the port number.
Foreign Address	Remote address and port number. The number after the last colon is the port number.
PMTU	Path MTU.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.11 show ipv6 tcp port

Use this command to display the current IPv6 TCP port status.

show ipv6 tcp port [*num*]

Parameter Description

Parameter	Description
<i>num</i>	Port number

Defaults N/A

Command Privileged EXEC mode
Mode

Usage Guide N/A

Configuration The following example displays the current IPv6 TCP port status.

Examples

```
Ruijie#show ipv6 tcp port
TCP connections on port 23:
Number Local Address Foreign Address State
1 1000::1:23 1000::2:64571 ESTABLISHED
Total: 1

TCP connections on port 2650:
Number Local Address Foreign Address State
Total: 0
```

Field	Description
Number	Number
Local Address	Local address and port number.
Foreign Address	Remote address and port number.
State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.
Process Name	Process name

The following example displays the current IPv6 TCP connection statistics.

```
Ruijie#show ipv6 tcp connect statistics
```

```

State          Count
-----
ESTABLISHED  1
SYN_SENT      0
SYN_RECV      0
FIN_WAIT1     0
FIN_WAIT2     0
TIME_WAIT     0
CLOSED        0
CLOSE_WAIT    0
LAST_ACK      0
LISTEN        1
CLOSING       0
Total: 2
    
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

11.12 show tcp connect

Use this command to display basic information about the current TCP connections.

show tcp connect [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]

Use this command to display the current IPv4 TCP connection statistics.

show tcp connect statistics

Parameter Description

Parameter	Description
local-ip <i>a.b.c.d</i>	Local IP address.
local-port <i>num</i>	Local port.
peer-ip <i>a.b.c.d</i>	Peer IP address.
peer-port <i>num</i>	Peer port.
statistics	Displays IPv4 TCP connection statistics.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the current IPv4 TCP connection information.

Examples

```
Ruijie#show tcp connect
Number Local Address      Foreign Address      State      Process name
1      0.0.0.0:22             0.0.0.0:0           LISTEN     rg-sshd
2      0.0.0.0:23             0.0.0.0:0           LISTEN     rg-telnetd
3      1.1.1.1:23             1.1.1.2:64201       ESTABLISHED rg-telnetd
```

Field	Description
Number	Sequence number.
Local Address	The Local address and port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23", "23" is the port number.
Foreign Address	The remote address and port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23", "23" is the port number.
State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.
Process name	Process name.

The following example displays the current IPv4 TCP connection statistics.

```
Ruijie#show tcp connect statistics
State      Count
-----
```

```

ESTABLISHED 1
SYN_SENT    0
SYN_RECV    0
FIN_WAIT1   0
FIN_WAIT2   0
TIME_WAIT   0
CLOSED      0
CLOSE_WAIT  0
LAST_ACK    0
LISTEN      1
CLOSING     0
Total: 2

```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

11.13 show tcp parameter

Use this command to show TCP parameters.

show tcp parameter

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows TCP parameters.

Examples

```

Ruijie#show tcp parameter
Hash table information:
  Established hash bucket size: 16384
  Bind hash bucket size: 16384
Memory information:
  Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages)

```



```

Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit:
bytes)
Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit:
bytes)
Current allocated memory: 0
Current memory pressure flag: 0
SYN specific information:
Max SYN_RECV sockets per LISTEN socket: 65535
Max SYN retries: 5
Max SYN ACK retries: 5
Timewait specific information:
Max timewait sockets: 180000
Current timewait sockets: 0
Timewait recycle: 0
Reuse timewait port: 0
Keepalive information:
Keepalive on: 0
Idle period: 900 seconds
Interval: 75 seconds
Max probes: 6
MTU probing:
Enable mtu probing: 0
FIN specific information:
FIN_WAIT_2 timeout: 60 seconds
Orphan socket information:
Max orphans: 16384
Max orphan retries: 0
Current orphans: 0
    
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

11.14 show tcp pmtu

Use this command to display information about TCP PMTU.
show tcp pmtu [local-ip a.b.c.d] [local-port num] [peer-ip a.b.c.d] [peer-port num]

Parameter Description	Parameter	Description
	local-ip a.b.c.d	Local IP address.

local-port <i>num</i>	Local port.
peer-ip <i>a.b.c.d</i>	Peer IP address.
peer-port <i>num</i>	Peer port.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays PMTU of IPv4 TCP connection.

Examples

```
Ruijie# show tcp pmtu
Number  Local Address          Foreign Address          PMTU
1       192.168.195.212.23     192.168.195.112.13560  1440
```

Field	Description
Number	Sequence number.
Local Address	The local address and the port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23", "23" is the port number.
Foreign Address	The remote address and the port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23", "23" is the port number.
PMTU	PMTU value.

Related Commands

Command	Description
ip tcp path-mtu-discovery	Enables the TCP PMTU discovery function.

Platform N/A

Description

11.15 show tcp port

Use this command to display information about the current TCP port.

show tcp port [*num*]

Parameter Description

Parameter	Description
<i>num</i>	Port number

Defaults N/A

Command Privileged EXEC mode
Mode

Usage Guide N/A

Configuration The following example displays the current IPv4 TCP port status.

Examples

```
Ruijie#sh tcp port
tcp port status:
Tcpv4 listen on 2650 have connections:
TCB          Foreign Address          Port      State
Tcpv4 listen on 2650 have total 0 connections.
Tcpv4 listen on 23 have connections:
TCB          Foreign Address          Port      State
c340800     1.1.1.2                  64571    ESTABLISHED
Tcpv4 listen on 23 have total 1 connections.
Tcpv6 listen on 23 have connections:
TCB          Foreign Address          Port      State
c429980     3000::2                  64572    ESTABLISHED
```

Tcpv6 listen on 23 have total 1 connections.

Field	Description
TCB	The control block's location in the current memory
Foreign Address	Remote address
Port	Remote port number
State	<p>Status of the current TCP connection. There are eleven possible states:</p> <p>CLOSED: The connection has been closed.</p> <p>LISTEN: Listening state</p> <p>SYNSENT: In the three-way handshake phase when the SYN packet has been sent.</p> <p>SYNRCVD: In the three-way handshake phase when the SYN packet has been received.</p> <p>ESTABLISHED: The connection has been established.</p> <p>FINWAIT1: The local end has sent the FIN packet.</p> <p>FINWAIT2: The FIN packet sent by the local end has been acknowledged.</p> <p>CLOSEWAIT: The local end has received the FIN packet from the peer end.</p> <p>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.</p> <p>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is</p>

	<p>received.</p> <p>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.</p>
--	---

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

11.16 show tcp statistics

Use this command to show TCP statistics on received packets, three way handshake and time-wait.

show tcp statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example shows TCP parameters.

Examples

```
Ruijie#show tcp statistics
TCP Packets
  Received: 1103
  Errors : 0(checksum: 0)
Three way handshake
  Request queue overflow: 0
  Accept backlog full: 0
  Web authentication limit per user: 0
  Failed to alloc memory for request sock: 0
  Failed to create open request child: 0
  SYN ACK retransmits: 0
  Timeouted requests: 0
Time-wait
  Time-wait bucket table overflow: 0
```

Field Description

Field	Description
TCP Packets	Normal packets and error packets
Three way handshake	Three way handshake information, including session request count, server-client connection count, three way handshake failure count caused by Web authentication limit, TCP socket failure count caused by memory shortage, sub-session failure count, packet retransmission count and session failure count caused by retransmission timeout.
Time-wait	Session in TIMEWAIT state

Related
Commands

Command	Description
N/A	N/A

Platform
Description

N/A

12 IPv4/IPv6 REF Commands

12.1 clear ip ref packet statistics

Use this command to clear IPv4 Ruijie Express Forwarding (REF) packet statistics.

clear ip ref packet statistics

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears IPv4 REF packet statistics.

```
Ruijie #clear ip ref packet statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

12.2 clear ipv6 ref packet statistics

Use this command to clear IPv6 REF packet statistics.

clear ipv6 ref packet statistics

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears IPv6 REF packet statistics.

Examples Ruijie #clear ipv6 ref packet statistics

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

12.3 show ip ref adjacency

Use this command to display the information about the specified adjacent node or all adjacent nodes.

show ip ref adjacency [glean | local | *ip-address* | interface *interface_type interface_number* | discard | statistics]

Parameter	Parameter	Description
Description	glean	Aggregate adjacent node, which is used for a direct route
	local	Local adjacent node, which is used by the local host
	<i>ip-address</i>	Next-hop IP address
	<i>interface_type</i>	Interface type
	<i>interface_number</i>	Interface number
	discard	Displays discarded adjacent nodes.
	statistics	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display the information about the adjacent node table in the current REF module. By specifying parameters, the information about the aggregate adjacent node, local adjacent node, adjacent node of the specified IP address, adjacent node associated with the specified interface, and all adjacent nodes can be displayed.

Configuration The following example displays the information about all adjacent nodes in the adjacent node table.

Examples

```
Ruijie#show ip ref adjacency
id state      type  rfct chg ip          interface          linklayer(header data)
1  unresolved mcast  1    0   224.0.0.0
9  resolved   forward 1    0   192.168.50.78 GigabitEthernet 0/0 00 25 64 C5 9D 6A 00 D0
F8 98 76 54 08 00
7  resolved   forward 1    0   192.168.50.200 GigabitEthernet 0/0 00 04 5F 87 69 66 00 D0
F8 98 76 54 08 00
6  unresolved glean   1    0   0.0.0.0          GigabitEthernet 0/0
```

```
4 unresolved local 3 0 0.0.0.0 Local 1
```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands	Command	Description
	show ip ref route	Displays all route information in the current REF module.

Platform N/A

Description

12.4 show ip ref exact-route

This command is used to display the IPv4 REF exact route.

```
show ip ref exact-route [ oob | vrf vrf_name ] source_ipaddress dest_ipaddress
```

Parameter Description	Parameter	Description
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	vrf vrf_name	VRF name, supported only by the VRF-supported device.
	<i>source_ipaddress</i>	Source IP address of the packet
	<i>dest_ipaddress</i>	Destination IP address of the packet

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to specify the source and the destination IP address of the IP packets, and to display the path of forwarding the current packet with REF

Configuration Examples The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.

```
Ruijie# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74 --> 192.168.13.1 (vrf global):
id state   type   rfct chg ip           interface      linklayer(header
data)
9  resolved forward 1     0   192.168.17.1 GigabitEthernet 0/0 00 25 64 C5 9D
6A 00 D0 F8 98 76 54 08 00
```

Description of fields:

Field	Description
id	Adjacency ID
state	Adjacency state: Unresolved Resolved
type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacency
chg	Whether the adjacency is on the changing link.
ip	Adjacency IP address
interface	Interface
linklayer	Layer 2 head

Related Commands	Command	Description
	show ip ref route	Displays all routing information in the current REF module.

Platform Description N/A

12.5 show ip ref packet statistics

Use this command to display IPv4 REF packet statistics.

show ip ref packet statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays IPv4 REF packet statistics.

Examples

```
Ruijie #show ip ref pkt-statistic
ref packet statistic:
  bad head      : 0
  lookup fib fail : 0
  local adj     : 0
  glean adj    : 0
  forward      : 0
  redirect     : 0
  punt adj     : 0
  outif not in ef : 0
  ttl expiration : 0
  no ip routing  : 0
```

Field	Description
total recved	Number of total packets received by REF
bad head	Number of the packets with false header
lookup fib fail	Number of the packets with failed REF routing
drop adj	Number of the packets matching the dropped adjacency
local adj	Number of the packets matching the local adjacency
glean adj	Number of the packets matching the gleaned adjacency
forward	Number of the packets matching the forwarded adjacency
no ip routing	Number of the packets not allowed to be forwarded and sent to local.

Related	Command	Description
---------	---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

12.6 show ip ref resolve-list

Use this command to display the IPv4 REF resolution information.

show ip ref resolve-list

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays IPv4 REF resolution information.

Examples

```
Ruijie#show ip ref resolve-list
IP                res_state flags interface
1.1.1.1          unres    1    GigabitEthernet 0/0
```

Field	Description
IP	IP address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

12.7 show ip ref route

Use this command to display all the routing information in the IPv4 REF table.

show ip ref route [oob | vrf vrf_name] [default | ip mask | statistics]

Parameter Description	Parameter	Description
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	vrf <i>vrf_name</i>	VRF name, supported only by the VRF-supported device.
	default	Specifies the default route.
	<i>ip</i>	Specifies the destination IP address of the route
	<i>mask</i>	Specifies the mask of the route.
	statistics	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the related routing information on the current REF table, and specify the default route and all the routing information matching IP/MASK.

Configuration Examples The following example displays all the routing information in the IPv4 REF table.

```
Ruijie#show ip ref route
Codes: * - default route
       # - zero route

ip      mask      weight path-id  next-hop  interface
255.255.255.255 255.255.255.255 1 4 0.0.0.0 Local 0
224.0.0.0      240.0.0.0      1 1 224.0.0.0
224.0.0.0      255.255.255.0  1 4 0.0.0.0 Local 0
192.168.50.0   255.255.255.0  1 6 0.0.0.0 FastEthernet 0/0
192.168.50.255 255.255.255.255 1 2 0.0.0.0
192.168.50.200 255.255.255.255 1 7 192.168.50.200 FastEthernet 0/0
192.168.50.122 255.255.255.255 1 4 0.0.0.0 Local 0
192.168.50.78 255.255.255.255 1 9 192.168.50.78 FastEthernet 0/0
```

Field	Description
ip	Destination IP address
mask	Mask
path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Egress

Related	Command	Description
---------	---------	-------------

Commands	
show ip ref exact-route	Displays the accurate REF forwarding path of an IP packet.

Platform N/A

Description

12.8 show ipv6 ref adjacency

Use this command to display the information about the IPv6 adjacent node.

show ipv6 ref adjacency [glean | local | ipv6-address | interface interface_type interface_number | discard | statistics]

Parameter	Parameter	Description
Description	glean	Aggregate adjacent node, which is used for a direct route
	local	Local adjacent node, which is used by the local host
	<i>ipv6-address</i>	Next-hop IP address
	<i>interface_type</i>	Interface type
	<i>interface_number</i>	Interface number
	discard	Displays discarded adjacent nodes.
	statistics	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display the information about the adjacent node table in the privileged EXEC mode and global configuration mode.

Configuration The following example displays the information about the IPv6 adjacent node..

Examples

```
Ruijie#show ipv6 ref adjacency
id   state      type   rfct  chg ip   interface          linklayer (header
data)
1    unresolved  glean  1     0   ::   GigabitEthernet 0/0
2    unresolved  local  2     0   ::1  Local 1
```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved

type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer(header data)	Layer 2 head

For distributed routers, id is divided into two fields, namely, gid and lid, standing for global adjacent node ID and local adjacent node ID respectively.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

12.9 show ipv6 ref exact-route

This command is used to display the IPv6 REF exact route.

show ipv6 ref exact-route [oob | vrf vrf_name] source-ipv6-address destination-ipv6-address

Parameter Description	Parameter	Description
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	vrf vrf_name	VRF name, supported only by the VRF-supported device.
	source-ipv6-address	Source IP address of the packet
	destination-ipv6-address	Destination IP address of the packet

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv4 REF exact route from 2001:db8:1::1 to 3001:db8:2::2.

```
Ruijie#show ipv6 exact-route 2001:db8:1::1 3001:db8:2::2
2001:db8:1::1 --> 3001:db8:2::2 (vrf global):
ID state      type      rfct chg ip interface          linklayer(header data)
3  unresolve  glean    1    0  :: GigabitEthernet 0/0
```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

12.10 show ipv6 ref packet statistics

Use this command to display IPv6 REF packet statistics.

show ipv6 ref packet statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays IPv6 REF packet statistics.

Examples

```
Ruijie#show ipv6 ref packet statistics
ref packet statistic:
  bad head      : 0
  lookup fib fail : 0
  local adj     : 0
  glean adj     : 0
  forward      : 0
  redirect      : 0
  hop-limit expiration : 0
  no ipv6 unicast-routing : 0
```

Field	Description
total recved	Number of total packets received by REF
bad head	Number of the packets with false header
lookup fib fail	Number of the packets with failed REF routing
drop adj	Number of the packets matching the dropped adjacency
local adj	Number of the packets matching the local adjacency
glean adj	Number of the packets matching the gleaned adjacency
forward	Number of the packets matching the forwarded adjacency
no ip routing	Number of the packets not allowed to be forwarded and sent to local.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

12.11 show ipv6 ref resolve-list

This command is used to display the IPv6 REF resolution information.

show ipv6 ref resolve-list

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration Examples The following example displays IPv6 REF resolution information.

```
Ruijie#show ipv6 ref resolve-list
IP           res_state flags interface
1000::1      unres     1     GigabitEthernet 0/0
```

Field	Description
IP	IPv6 address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.12 show ipv6 ref route

Use this command to display all the routing information in the IPv6 REF table.

show ipv6 ref route [oob | vrf *vrf-name*] [default | statistics | prefix/len]

Parameter Description	Parameter	Description
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	vrf <i>vrf_name</i>	VRF name, supported only by the VRF-supported device.
	default	Specifies the default route.
	statistics	Statistics

prefix/len	Displays the route with the specified prefix (X:X:X:X:<0-128>).
------------	---

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display all routing information in the IPv6 REF table. If there is no VRF parameter, information about the global REF table is displayed; if there is VRF parameter, information about the specified VRF table is displayed. The command can also be used to display information about the default route, the route with the specified prefix, and statistics of all types of routes.

Configuration The following example displays all the routing information in the REF IPv6 table.

Examples

```
Ruijie#show ipv6 ref route
Codes: * - default route
prefix/len                weight path_id next_hop interface
2001:da8:ffe:2::/64       1      3      ::      GigabitEthernet 0/0
2001:da8:ffe:2::3/128    1      2      :::1    Local 1
fe80::/10                 1      6      ::      Null 0
fe80::21a:a9ff:fe3b:fa41/128 1      2      :::1    Local 1
```

Field	Description
prefix/len	IPv6 prefix and prefix length.
path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A



IP Routing Commands

1. RIP Commands
2. OSPFv2 Commands
3. OSPFv3 Commands
4. IS-IS Commands
5. BGP4 Commands
6. PBR Commands
7. VRF Commands
8. RIPng Commands
9. NSM Commands
10. Protocol-independent Commands

1 RIP Commands

1.1 address-family

Use this command to configure the RIP protocol in address family configuration sub-mode. Use the **no** form of this command to restore the default setting.

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf-name*

Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	Specifies the VRF name associated with the sub-mode command.

Defaults The address family of the RIP protocol is not configured by default.

Command Mode Route configuration mode

Usage Guide Use the **address-family** command to enter the address family configuration sub-mode. The prompt is (config-router-af) #. When you specify the VRF associated with the sub-mode for the first time, the RIP instance corresponding to the VRF will be created. In the sub-mode, you can configure the VRF RIP routing information.

To remove the address family sub-mode and return to the route configuration mode, use the **exit-address-family** or **exit** command.

Configuration Examples The following example creates a VRF with the name of vpn1 and creates its RIP instance.

```
Ruijie(config)# ip vrf vpn1
Ruijie(config-vrf)# exit
Ruijie(config)# interface fastEthernet 1/0
Ruijie(config-if-FastEthernet 0/1)# ip vrf forwarding vpn1
Ruijie(config-if-FastEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Ruijie(config)# router rip
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router)# network 192.168.1.0
Ruijie(config-router)# exit-address-family
```

Related Commands	Command	Description
	exit-address-family	Exits the address family configuration sub-mode.
	ip vrf	Creates a VRF.

Platform N/A

Description

1.2 auto-summary

Use this command to enable automatic summary of RIP routes. Use the **no** form of this command to disable this function

auto-summary

no auto-summary

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Automatic summary of RIP routes is enabled by default

Command


Mode Routing progress configuration mode

Usage Guide Automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classified network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.

Automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly.

Advertising the summarized route is more efficient than advertising individual routes in light of the following factors:

- The summarized route is always processed preferentially when you query the RIP database.
- Any sub-route is ignored when you query the RIP database, reducing the processing time.
- If you want to learn the specific sub-routes instead of the summarized route, disable the automatic route summary function. Only when RIPv2 is configured, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

 The range of the supernet route is wider than that of the classful network. Therefore, this command takes no effect on the supernet route.

Configuration The following example disables automatic route summary of RIPv2.

```
Examples Ruijie (config)# router rip
Ruijie (config-router)# version 2
Ruijie (config-router)# no auto-summary
```

Related Commands	Command	Description
	version	Defines the RIP software versions: v1 or v2. Both v1 and v2 are supported by default.

Platform N/A
Description

1.3 bdf all-interfaces

Use this command to enable all interfaces running RIP to use the BDF function. Use the **no** form of this command to restore the default setting.

bdf all-interfaces

no bdf all-interfaces

Parameter Description	Parameter	Description
	N/A	N/A

Defaults BFD is not configured by default.

Command Mode Routing process configuration mode

Usage Guide With the BFD function enabled on the RIP, one BFD session will be established for the RIP routing information source (the source address of the RIP route update packet). Once the BFD neighbor fails, the RIP routing information will be invalid directly and no longer join routing or forwarding. You can also use the interface configuration mode command **ip rip bfd [disable]** to enable or disable the BFD function on the specified interface, which takes precedence over the command **bdf all-interfaces** in the routing process configuration mode.

Configuration

Examples N/A

Related Commands	Command	Description
	route ip	Creates the RIP routing process and enters the routing process configuration mode.
	ip rip bfd [disable]	Configures a specified interface running RIP to enable or disable link detection using the BFD.

Platform N/A
Description

1.4 default-information originate

Use this command to generate a default route in the RIP process. Use the **no** form of this command to delete the generated default route.

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Enables RIP to generate the default route, no matter whether the default route exists or not.
metric <i>metric-value</i>	(Optional) The original metric value of the default route with the value range 1-15 of metric-value.
route-map <i>map-name</i>	(Optional) Name of the associated route-map. Route-map is not associated by default.

Defaults

No default route is generated by default.

The default metric value is 1.

Command

Mode

Routing process configuration mode


Usage Guide


By default, RIP will not advertise the default route if the default route exists in the routing table of the router. In this case, use the **default-information originate** command to notify the neighbor of the default route.

With the parameter **always** configured, no matter whether the default route exists in the RIP routing process or not, the default route will be advertised to the neighbor but is not shown in the local routing table. You can use the **show ip rip database** command to view the RIP routing information database to confirm whether the default route is generated.

Use the parameter **route-map** to control more about the default route advertised to RIP. For example, use the **set metric** command to set the metric value of the default route.

The route-map set metric rule takes precedence over the parameter metric value configuration of the default route. If the parameter metric is not configured, the default metric value is used by the default route.

 If the default route can be generated in the RIP process by using this command, RIP will not learn the default route advertised from the neighbor.

 For the default route generated by using the `ip default-network` command, the `default-information originate` command is required to add the default route to RIP.

Configuration

The following example generates a default route to the RIP routing table.

Examples

```
Ruijie(config-router)# default-information originate always
```

Related

Command	Description
---------	-------------

Commands	
ip rip default-information	Notifies the default route through an interface.
redistribute	Redistributes the routes from other protocols to RIP.

Platform N/A

Description

1.5 default-metric

Use this command to define the default RIP metric value. Use the **no** form of this command to restore the default setting.

default-metric *metric-value*

no default-metric

Parameter Description	Parameter	Description
	<i>metric-value</i>	Indicates the default metric value with the range from 1 to 16. If the metric value is greater than or equal to 16, the RGOS regards the route unreachable.

Defaults The default is 1.

Command

Mode Routing process configuration mode

Usage Guide This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric value cannot be converted due to the incompatibility of the metric calculation mechanisms for different protocols. During the conversion, therefore, it is required to redefine the metric values of redistributed routes in the RIP routing domain. If there is no clear definition of the metric value in redistributing a routing protocol process, the RIP uses the metric value defined with **default-metric**. If the metric value is defined, this value overwrites the metric value defined with **default-metric**. If this command is not configured, the default value of **default-metric** is 1.

Configuration Examples The following example enables the RIP routing protocol to redistribute the routes learned by the OSPF routing protocol, whose initial RIP metric value is set to 3.

```
Ruijie (config)# router rip
Ruijie (config-router)# default-metric 3
Ruijie (config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the routes from one routing

	domain to another routing domain.
--	-----------------------------------

Platform N/A

Description

1.6 distance

Use this command to set the management distance of the RIP route. Use the **no** form of this command to restore the default setting.

distance *distance* [*ip-address wildcard*]

no distance [*distance ip-address wildcard*]

Parameter Description	Parameter	Description
	<i>distance</i>	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
	<i>ip-address</i>	Indicates the prefix of the source IP address of the route.
	<i>wildcard</i>	Defines the comparison bit of the IP address, where 0 means accurate matching and 1 means no comparison.

Defaults The default is 120.

Command

Mode Routing process configuration mode

Usage Guide Use this command to set the management distance of the RIP route. You can use this command to create several management distances with source address prefixes. When the source address of the RIP route is within the range specified by the prefixes, the corresponding management distance is applied; otherwise, the route uses the management distance configured by the RIP.

Configuration The following example sets the management distance of the RIP route to 160, and specifies the

Examples management distance of the route learned from 192.168.2.1 as 123.

```
Ruijie(config)# router rip
Ruijie(config-router)# distance 160
Ruijie(config-router)# distance 123 192.168.12.1 0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.7 distribute-list in

Use this command to control route update for route filtering. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type* *interface-number*]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type* *interface-number*]

Parameter Description	Parameter	Description
	<i>access-list-number</i> <i>name</i>	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
	prefix <i>prefix-list-name</i>	Uses the prefix list to filter the routes.
	gateway <i>prefix-list-name</i>	Uses the prefix list to filter the source of the routes.
	<i>interface-type</i> <i>interface-number</i>	(Optional) Applies the distribution list only to a specified interface.

Defaults The distribution list is not defined by default.

Command Mode Routing process configuration mode

Usage Guide To deny receiving some specified routes, you can process all the received route update packets by configuring the route distribute control list.
Without any interface specified, the system will process the route update packets received on all the interfaces.

Configuration Examples The following example enables RIP to control the routes received from the FastEthernet 0/0, only permitting the routes starting with 172.16.

```
Ruijie (config)# router rip
Ruijie (config-router)# network 200.168.23.0
Ruijie (config-router)# distribute-list 10 in fastethernet 0/0
Ruijie (config-router)# no auto-summary
Ruijie (config-router)# access-list 10 permit 172.16.0.0 0.0.255.255
```

Related Commands	Command	Description
	access-list	Defines the ACL rule.
	prefix-list	Defines the prefix list.

Platform Description N/A

1.8 distribute-list out

Use this command to control route update advertisement for filtering routes. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* [[**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* [[**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]]

Parameter Description

Parameter	Description
<i>access-list-number</i> <i>name</i>	Specifies the ACL.
prefix <i>prefix-list-name</i>	Uses the prefix list to filter routes.
<i>interface</i>	(Optional) Applies route update advertisement control to a specified interface in the distribution list.
bgp	(Optional) Applies route update advertisement control to only routes introduced from bgp in this distribution list.
connected	(Optional) Applies route update advertisement control to only connected routes in this distribution list.
isis [<i>area-tag</i>]	(Optional) Applies route update advertisement control to only routes introduced from ISIS in this distribution list. <i>area-tag</i> specifies an ISIS instance.
ospf <i>process-id</i>	(Optional) Applies route update advertisement control to only routes introduced from OSPF in this distribution list. <i>process-id</i> specifies an OSPF instance.
rip	(Optional) Applies route update advertisement control to only RIP routes in this distribution list.
static	(Optional) Applies route update advertisement control to only static routes in this distribution list.

Defaults No route update advertisement is configured by default.

Command

Mode Routing process configuration mode

Usage Guide If this command relates to none of optional parameters, route update advertisement control applies to all interfaces. If this command relates to interface options, route update advertisement control applies to only the specified interface. If this command relates to other route process parameters, route update advertisement control applies to only the specific route process.

Configuration The following example advertises only the 192.168.12.0/24 route.

Examples

```
Ruijie (config)# router rip
Ruijie (config-router)# network 200.4.4.0
Ruijie (config-router)# network 192.168.12.0
```

```
Ruijie (config-router)# distribute-list 10 out
Ruijie (config-router)# version 2
Ruijie (config-router)#access-list 10 permit 192.168.12.0 0.0.0.255
```

**Related
Commands**

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.
redistribute	Configures route redistribution.

Platform N/A
Description

1.9 enable mib-binding

Use this command to bind a MIB with a specified RIP instance. Use the **no** form of this command to restore the default setting

enable mib-binding

no enable mib-binding

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults By default, the MIB is bound with the RIP instance of the default VRF.

Command

Mode Routing process configuration mode.

Usage Guide As RIP MIB does not have RIP instance information, you can only operate only one RIP instance using SNMP. By default, RIP MIB is bound with the RIP instance of the default VRF. You can only operate this RIP instance. If you want to operate another RIP instance of a specified VRF through SNMP, you can use this command to bind the MIB with this instance.

Configuration The following example operates the RIP instance of a specified VRF, vpn1.

Examples

```
Ruijie(config)# router rip
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router-af)# enable mib-binding
```

**Related
Commands**

Command	Description
show ip rip	Displays the global configuration of RIP.

Platform N/A

Description

1.10 exit-address-family

Use this command to exit the address family configuration mode

exit-address-family

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command

Mode Address family configuration mode

Usage Guide Use this command to exit the address family configuration mode.
The abbreviation of this command is exit.

Configuration The following example enters or exits the address family configuration mode.

Examples

```
Ruijie(config-router)# address-family ipv4 vrf vpn1
```

```
Ruijie(config-router-af)# exit-address-family
```

Related Commands	Command	Description
	address-family	Enters the address family configuration sub-mode.

Platform N/A

Description

1.11 fast-reroute

Use this command to enable the RIP FRR (Fast Reroute) function for the device. Use the **no** form of this command to restore the default setting.

fast-reroute route-map *route-map-name*

no fast-reroute

Parameter Description	Parameter	Description
	<i>route-map-name</i>	Specifies the backup path through the route map.

Defaults This function is disabled by default.

Command**Mode** Routing process configuration mode

Usage Guide Use the **route-map** command to specify the backup path for the matched routes. It is recommended to enable the BFD function when the RIP fast reroute function is enabled. BFD allows the device to detect the link fault faster, so as to reduce the interruption time. In the scenario where the port is up/down, it is recommended to configure **carrier-delay 0** in interface configuration mode to achieve the fastest switchover speed, reducing the interruption time.

Currently, the restrictions of the RIP FRR are as follows:

- Only one backup next hop is generated for each route.
- The backup next hop is not generated for the ECMP route.

Configuration The following example enables FRR for RIP instance 1 and associates route map *fast reroute*.

Examples

```
Ruijie(config)# route-map fast-reroute
match interface gigabitEthernet 0/2
set fast-reroute backup-interface GigabitEthernet 0/1 backup-nexthop
192.168.1.1
Ruijie(config)# router rip
Ruijie(config-router)# fast-reroute route-map fast-reroute
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.12 graceful-restart

Use this command to configure the RIP graceful restart (GR) function for a device. Use the **no** form of this command to restore the default configuration.

graceful-restart [**grace-period** *grace-period*]**no graceful-restart** [**grace-period**]**Parameter Description**

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	(Optional) Configures the grace period.
<i>grace-period</i>	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The range is from 1 to 1,800. The unit is second.

Defaults This function is enabled by default.


Command

Mode Routing process configuration mode

Usage Guide The GR function is configured on the RIP instances. Different parameters can be configured for different RIP instances.

The GR period refers to the time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation.

The **graceful-restart grace-period** command enables users to modify GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If an improper value is configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the period needs to changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the **timers basic** command.

 During the RIP GR period, the network must be stable.

Configuration Examples The following example enables the RIP GR function and configures the GR period parameters of the GR function.

```
Ruijie(config)# router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

Related Commands

Command	Description
timers basic	Configures RIP timers.

Platform N/A
Description

1.13 ip rip authentication key-chain

Use this command to enable RIP authentication and specify the keychain used for RIP authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication key-chain *name-of-keychain*

no ip rip authentication key-chain

Parameter

Parameter	Description
-----------	-------------

Description	
	<i>name-of-keychain</i> Indicates the name of the keychain, which specifies the keychain used for RIP authentication.

Defaults The keychain is not associated by default.

Command

Mode Interface configuration mode

Usage Guide If the keychain is specified in the interface configuration, use the key chain global configuration command to define the keychain. Otherwise, RIP data packet authentication fails. RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples The following example enables RIP authentication on the fastEthernet 0/1 with the associated keychain ripchain.

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)#ip rip authentication key-chain ripchain
Meanwhile, use the key chain command to define this keychain in global configuration mode.
Ruijie(config)#key chain ripchain
Ruijie(config-keychain)#key 1
Ruijie(config-keychain-key)#key-string Hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication text-password	Enables RIP authentication, and sets the password string of RIP plaintext authentication. RIP data packet authentication is supported only by RIPv2.
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
key chain	Defines the keychain and enters keychain configuration mode.

Platform Description N/A

1.14 ip rip authentication mode

Use this command to define the RIP authentication mode. Use the **no** form of this command to restore the default setting.

ip rip authentication mode { text | md5 }

no ip rip authentication mode**Parameter
Description**

Parameter	Description
text	Configures RIP authentication as plaintext authentication.
md5	Configures RIP authentication as MD5 authentication.

Defaults

It is plaintext authentication by default.

Command**Mode**

Interface configuration mode

Usage Guide

During the RIP authentication configuration process, the RIP authentication modes of all devices requiring exchange of RIP routing information must be the same. Otherwise, RIP packet exchange will fail.

If the plaintext authentication mode is adopted, but the password string of the plaintext authentication or the associated keychain is not configured, no authentication occurs. In the same way, if the MD5 authentication mode is adopted, but the associated keychain is not configured, no authentication occurs.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration

The following example configures the RIP authentication mode on the fastEthernet 0/1 as MD5.

Examples

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip authentication mode md5
```

**Related
Commands**

Command	Description
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication of the RIP data packet.
ip rip authentication text-password	Enables the RIP authentication mode, and sets the password string of RIP plaintext authentication. Only RIPv2 supports authentication of the RIP data packet.
key chain	Defines the keychain and enters the keychain configuration mode

Platform

N/A

Description

1.15 ip rip authentication text-password

Use this command to enable RIP authentication and set the password string of RIP plaintext

authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication text-password [0 | 7] *password-string*

no ip rip authentication text-password

Parameter Description	Parameter	Description
	0	Specifies that the key is displayed as plaintext.
	7	Specifies that the key is displayed as cipher text.
	<i>password-string</i>	Indicates the password string of the plaintext authentication, in the length of 1-16 bytes.

Defaults No password string of RIP plaintext authentication is configured by default.

Command

Mode Interface configuration mode

Usage Guide

This command works only in plaintext authentication mode.

To enable the RIP plaintext authentication function, use this command to configure the corresponding password string, or use the associated key chain to obtain the password string. The latter takes the precedence over the former one.

RIPv1 does not support RIP authentication but RIPv2 does.

Configuration Examples The following example enables the RIP plaintext authentication on fastEthernet 0/1 and sets the password string to hello.

```
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip authentication text-password hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication.

Platform N/A

Description

1.16 ip rip bfd

Use the **ip rip bfd** [**disable**] command to configure the specified interface running RIP to enable or disable link detection using the BFD. Use the **no** form of this command to restore the default setting.

ip rip bfd [**disable**]

no ip rip bfd

Parameter Description	Parameter	Description
	disable	Disables the specified interface running RIP and uses the BFD mechanism to perform link detection.

Defaults Interfaces running RIP are not configured by default. The BFD configuration in RIP process configuration mode is a reference.

Command

Mode Interface configuration mode

Usage Guide The priority of the interface is higher that of the `bfd all-interfaces` command in process configuration mode.

You can use the `ip rip bfd` command to enable the BFD to perform link detection on the specified interface according to the actual environment or use the `bfd all-interfaces` command to configure all interfaces running RIP and enable the BFD to perform link detection. In addition, you can use the `ip rip bfd disable` command to disable the BFD detection function on the specified interface.

Configuration

Examples N/A

Related Commands	Command	Description
	route ip	Enables the RIP routing process and enters the routing process configuration mode.
	bfd all-interfaces	Configures all interfaces running RIP to use the BFD to perform link detection.

Platform N/A

Description

1.17 ip rip default-information

Use this command to advertise the default route through a RIP interface. Use the **no** form of this command to restore the default setting.

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

no ip rip default-information

Parameter Description	Parameter	Description
	only	Notifies the default route rather than other routes.
	originate	Notifies the default route and other routes.


metric <i>metric-value</i>	Specifies the metric value of the default route, in the range from 1 to 15.
-----------------------------------	---

Defaults No default route is configured by default. The default metric value is 1.

Command

Mode Interface configuration mode

Usage Guide After you configure this command on a specified interface, a default route is generated and notified through the interface. If the **ip rip default-information** command of the interface and the **default-information originate** command of the RIP process are configured at the same time, only the default route of the interface is advertised.

 RIP will no longer learn the default route notified by the neighbor if any interface is configured with the ip rip default-information command.

Configuration The following example creates a default route which is notified on ethernet0/1 only.

Examples

```
Ruijie(config)#interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)#ip rip default-information only
```

Related Commands

Command	Description
default-information originate	Generates a default route in the RIP process.

Platform N/A

Description

1.18 ip rip receive enable

Use this command to enable RIP to receive the RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip receive enable

no ip rip receive enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP packages can be received through the interface by default.

Command

Mode Interface configuration mode

Usage Guide To prevent an interface from receiving RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to receive the RIP data package.

Configuration The following example prohibits receiving RIP data packages on fastEthernet 0/1.

Examples

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# no ip rip receive enable
```

Related Commands	Command	Description
	ip rip send enable	Enables or disables the interface to send RIP data packages.
passive-interface	Configures a passive RIP interface.	

Platform N/A

Description

1.19 ip rip receive version

Use this command to define the version of RIP packets received on an interface. Use the **no** form of this command to restore the default setting.

ip rip receive version [1] [2]

no ip rip receive version

Parameter Description	Parameter	Description
	1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.	

Defaults The default behavior depends on the configuration with the version command.

Command

Mode Interface configuration mode

Usage Guide This command overwrites the default configuration of the **version** command. It affects only RIP packet receiving through the interface and allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If the command is configured without parameters, data package receiving depends on the configuration of the version.

Configuration The following example enables receiving both RIPv1 and RIPv2 data packages.

Examples

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip receive version 1 2
```

Related	Command	Description
---------	---------	-------------

Commands	
version	Defines the default version of the RIP packets received/sent on the interface.

Platform N/A

Description

1.20 ip rip send enable

Use this command to enable RIP to send a RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip send enable

no ip rip send enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults RIP packages can be sent through the interface by default.

Command

Mode Interface configuration mode

Usage Guide To prevent an interface from sending RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to send the RIP data package.

Configuration The following example prohibits sending RIP data packages on fastEthernet 0/1.

Examples

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# no ip rip send enable
```

Related Commands	Command	Description
	ip rip receive enable	Enables or disables receiving RIP packets on the interface.
	passive-interface	Configures a passive RIP interface.

Platform N/A

Description

1.21 ip rip send supernet-routes

Use this command to enable RIP to send the supernet route on a specified interface. Use the **no** form

of this command to disable this function.

ip rip send supernet-routes

no ip rip send supernet-routes


Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command

Mode Interface configuration mode

Usage Guide When the RIPv1 router monitors a RIPv2 router response packet and if the supernet routing information is monitored, incorrect route information is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, you are advised to use the **no** form of this command on the RIPv2 router to disable advertising the supernet route on the corresponding interface. This command works only on interfaces configured with this command.

 This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet route.

Configuration The following example disables sending RIP supernet routes on the fastEthernet 0/1 interface.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip send supernet-routes
```

Related Commands

Command	Description
version	Defines the RIP version
ip rip send enable	Enables or disables sending the RIP package on the interface.

Platform N/A

Description

1.22 ip rip send version

Use this command to define the version of the RIP packets sent on the interface. Use the **no** form of this command to restore the default setting.

ip rip send version [1] [2]

no ip rip send version

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults The default behavior depends on the configuration with the version command.

Command

Mode Interface configuration mode

Usage Guide This command overwrites the default configuration of the **version** command. It affects only RIP packet sending through the interface and allows RIPv1 and RIPv2 packages sent on the interface at the same time. If the command is configured without parameters, package receiving depends on the configuration of the version.

Configuration Examples The following example enables sending both RIPv1 and RIPv2 packages on the fastEthernet 0/1 interface.

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip send version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interfaces.

Platform N/A
Description

1.23 ip rip split-horizon

Use this command to enable split horizon. Use the **no** form of this command to disable this function.

ip rip split-horizon [poisoned-reverse]

no ip rip split-horizon [poisoned-reverse]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables split horizon with poisoned reverse.

Defaults This function is enabled by default.

Command

Mode Interface configuration mode

Usage Guide When multiple devices are connected to the IP broadcast network and run a distance vector routing protocol, the split horizon mechanism is required to prevent loop. The split horizon prevents the

device from advertising routing information from the interface that learns that information, which optimizes routing information exchange between multiple devices.

For non-broadcast multi-path access networks (such as frame relay and X.25), split horizon may cause some devices to be unable to learn all routing information. Split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for split horizon.

If the **poisoned-reverse** parameter is configured, split horizon with poisoned reverse is enabled. In this case, devices still advertise the route information through the interface from which the route information is learned. However, the metric value of the route information is set to unreachable. The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, use the show ip rip command to judge. This function makes no influence on the neighbor defined with the **neighbor** command.

Configuration The following example disables the RIP split horizon function on the interface fastethernet 0/0.

Examples

```
Ruijie (config)# interface fastethernet 0/1
Ruijie (config-if)# no ip rip split-horizon
```

**Related
Commands**

Command	Description
neighbor (RIP)	Defines the IP address of the neighbor of RIP.
validate-update-source	Enables the source address authentication of the RIP route update message.

Platform N/A

Description

1.24 ip rip subvlan

Use this command to enable RIP on super VLANs. Use the **no** form of this command to restore the default setting.

ip rip subvlan [all | vid]

no ip rip subvlan

**Parameter
Description**

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults The default setting takes effect only on super VLANs with RIP disabled.

Command

Mode Interface configuration mode

Usage Guide In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIPng multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIPng multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the RIPng function does not need to be enabled on a super VLAN. Therefore, the RIPng function is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration The following example sends the RIP multicast packets to sub VLAN 1024 of super VLAN 300.

Examples

```
Ruijie(config)# interface vlan 300
Ruijie(config-if-VLAN 300)# ip rip subvlan 1024
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.25 ip rip summary-address

Use this command to configure port-level convergence through an interface. Use the **no** form of this command to disable this function.

ip rip summary-address *ip-address ip-network-mask*

no ip rip summary-address *ip-address ip-network-mask*

Parameter Description

Parameter	Description
<i>ip-address</i>	Indicates the IP addresses to be converged.
<i>ip-network-mask</i>	Indicates the subnet mask of the specified IP address for route convergence.


Defaults The RIP routes are automatically converged to the classful network edge by default.

Command

Mode Interface configuration mode

Usage Guide The **ip rip summary-address** command converges an IP address or a subnet on a specified port.

RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.

-  The summary range configured by this command cannot be a super class network, that is, the configured mask length is greater than or equal to the natural mask length of the network.

Configuration Examples The following example disables the automatic route convergence function of RIPv2. Interface convergence is configured so that fastEthernet 0/1 advertises the converged route 172.16.0.0/16.

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0
255.255.0.0
Ruijie (config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Ruijie (config)# router rip
Ruijie (config-router)# network 172.16.0.0
Ruijie (config-router)# version 2
Ruijie (config-router)# no auto-summary
```

Related Commands

Command	Description
auto-summary	Enables the automatic convergence of RIP routes.

Platform N/A

Description

1.26 ip rip triggered

Use this command to enable triggered RIP based on links. Use the **no** form of this command to restore the default setting.

ip rip triggered

ip rip triggered retransmit-timer *timer*

ip rip triggered retransmit-count *count*

no ip rip triggered

no ip rip triggered retransmit-timer

no ip rip triggered retransmit-count

Parameter Description

Parameter	Description
retransmit-timer <i>timer</i>	Configures the interval at which the Update Request and Update Response packets are retransmitted. The range is from 1 to 3,600. The unit is second. The default is five.
retransmit-count <i>count</i>	Configures the maximum times that the Update Request and Update Response packets are retransmitted. The range is from 1 to 3600. The default is 36.

Defaults This function is disabled by default.

Command

Mode Interface configuration mode

Usage Guide Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for demand-based links.

With the TRIP function enabled, RIP no longer sends route updates periodically and sends route updates to the WAN interface only if:


Update Request packets are received.


RIP routing information is changed.


Interface state is changed.


The router is started.


As periodical RIP update is disabled, the confirmation and retransmission mechanism is required to ensure that update packets are sent and received successfully over the WAN. The **retransmit-timer** and **retransmit-count** commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.


 The function can be enabled in the case of the following conditions: a) The interface has only one neighbor. b) There are multiple neighbors but they interact information using unicast packets. You are advised to enable the function for link layer protocols such as PPP, frame relay, and X.25.

 You are advised to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might be left.

 Make sure that the function is enabled on all routers on the same link; otherwise the function will be invalid and the routing information cannot be exchanged correctly.

 The function cannot be enabled at the same time with BFD and RIP functions.

 To enable the function, make sure that the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.

 If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source IP address verification function (validate-update-source) is enabled.

Configuration The following example enables TRIP and sets the retransmission interval and maximum

Examples retransmission time to 10 seconds and 18 respectively for Update Request and Update Response packets.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18
```

Related Commands	Command	Description
	show ip rip database	Displays the summarized routing information of the RIP database.
	show ip rip interface	Displays the RIP interface information.
	ip rip split-horizon	Configures RIP split horizon.

Platform N/A
Description

1.27 ip rip v2-broadcast

Use this command to send RIPv2 packets in broadcast rather than multicast mode. Use the **no** form of this command to restore the default setting.

ip rip v2-broadcast
no ip rip v2-broadcast

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The default behavior depends on the configuration of the version command.

Command

Mode Interface configuration mode

Usage Guide This command overwrites the default of the **version** command. This command affects only sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packages sent on the interface simultaneously. If this command is configured without parameters, package receiving depends on the version setting.

Configuration The following example sends RIPv2 packets in broadcast mode on the fastEthernet 0/1 interface.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip split-horizon
```

Related Commands	Command	Description
	version	Defines the default version of the RIP packets received and sent on the interface.

Platform N/A
Description

1.28 neighbor

Use this command to define the IP address of a RIP neighbor. Use the **no** form of this command to restore the default setting.

neighbor *ip-address*

no neighbor *ip-address*

Parameter Description	Parameter	Description
	<i>ip-address</i>	Indicates the IP address of the neighbor. The IP address must be that of the network connected to the local device.

Defaults The neighbor is not defined by default.

Command

Mode Routing process configuration mode

Usage Guide By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 uses the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, use the **passive-interface** command to configure related interfaces as passive interfaces and then define only some neighbors who can receive the routing information. This command has no impact on the receiving of RIP information. The passive interface is configured. No request packet is sent after the interface is enabled.

Configuration The following example creates a VRF with the name of vpn1 and creates its RIP instance.

```
Ruijie(config)# ip vrf vpn1
Ruijie(config-vrf)# exit
Ruijie(config)# interface fastEthernet 1/0
Ruijie(config-if-FastEthernet 0/1)# ip vrf forwarding vpn1
Ruijie(config-if-FastEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
Ruijie(config)# router rip
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router)# network 192.168.1.0
Ruijie(config-router)# exit-address-family
```

Related Commands	Command	Description
	passive-interface	Configures the interface as a passive interface.

Platform Description N/A

1.29 network

Use this command to define the list of networks to be advertised in the RIP routing process. Use the **no** form of this command to delete the defined network.

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter Description	Parameter	Description
	<i>network-number</i>	Indicates the network number of the directly-connected network. The network number is a natural one. All interfaces whose IP addresses belong to that natural network can send/receive RIP packages.
	<i>wildcard</i>	Defines the IP address comparing bit: 0 refers to accurate matching, and 1 refers to no comparison.

Defaults N/A

Command

Mode Routing process configuration mode

Usage Guide The *network-number* and *wildcard* parameters can be configured simultaneously to enable the IP address of the interface within the IP address range to join RIP running.

Without the *wildcard* parameter, RGOS make the interface IP address within the classful address range join the RIP running.

Only when the IP address of an interface is in the network list defined by RIP, RIP route update packets can be received and sent on the interface.

Configuration Examples The following example defines two network numbers associated with RIP and allows the interface IP address between 192.168.12.0/24 and 172.16.0.0/24 to join RIP running.

```
Ruijie (config)# router rip
Ruijie (config-router)# network 192.168.12.0
Ruijie (config-router)# network 172.16.0.0 0.0.0.255
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.30 offset-list

Use this command to increase the metric value of received or sent RIP routes. Use the **no** form of this

command to restore the default setting.

offset-list { access-list-number | name } { **in** | **out** } offset [interface-type interface-number]

no offset-list { access-list-number | name } { **in** | **out** } offset [interface-type interface-number]

Parameter Description	Parameter	Description
	<i>access-list-number name</i>	Specifies the ACL.
	in	Modifies the metric of the received routes using the ACL.
	out	Modifies the metric of the sent routes using the ACL.
	<i>offset</i>	Indicates the offset of changed metric values. The value is in the range from 0 to16.
	<i>interface-type</i>	Applies the ACL to a specified interface.
	<i>interface-number</i>	Specifies the interface number.

Defaults No offset is specified by default.

Command

Mode Routing process configuration mode

Usage Guide If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

Configuration The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7.

Examples Ruijie (config-router)# offset-list 7 out 7

The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastethernet 0/1.

Ruijie (config-router)# offset-list 8 in 7 fastethernet 0/1

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.31 output-delay

Use this command to modify the delay to send RIP update packets. Use the **no** form of this command to restore the default setting.

output-delay *delay*

no output-delay

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	<i>delay</i>	Sets the delay to send RIP update packets, in the range from 8 to 50 in the unit of milliseconds.

Defaults No sending delay is configured by default.

Command

Mode Routing process configuration mode

Usage Guide In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible.

However, when a high-speed device sends a large number of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Configuration The following example sets the delay to send RIP update packets to 30 milliseconds.

Examples

```
Ruijie(config)# router rip
Ruijie(config-router)# output-delay 30
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

1.32 passive-interface

Use this command to disable the function of sending update packets on an interface. Use the **no** form of this command to restore the default setting.

```
passive-interface { default | interface-type interface-num }
no passive-interface { default | interface-type interface-num }
```

Parameter Description	Parameter	Description
	default	Sets all interfaces to the passive interfaces.
	<i>interface-type interface-num</i>	Indicates the interface type and number.

Defaults Interfaces are set to the non passive interfaces by default.

Command Routing process configuration mode

Mode

Usage Guide The **passive-interface default** command sets all interfaces to the passive interfaces. You can use **no passive-interface** *interface-type interface-num* command to set specified interfaces as non-passive interfaces.

After you set an interface to the passive interface, RIP route update packets will no longer be sent but can be received through the interface. In this case, route update packets can be sent to a specified neighbor through the interfaces by using the **neighbor** command. You can use the **ip rip send enable** and **ip rip receive enable** commands to control whether route update packets can be sent or received through the interface.

Configuration Examples The following example sets all interfaces to the passive interfaces and then sets ethernet0/1 to the non-passive interface.

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface gigabitEthernet 0/1
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on the interface.
ip rip send enable	Enables or disables sending RIP packets on the interface.

Platform N/A
Description

1.33 redistribute

Use this command to redistribute external routes in route configuration mode. Use the **no** form of this command to restore the default setting.

```
redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | static } [ { level-1 | level-1-2 | level-2 } ] [ match { internal | external [ 1|2 ] | nssa-external [ 1|2 ] } ] [ metric metric-value ] [ route-map route-map-name ]
```

```
no redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | static } [ { level-1 | level-1-2 | level-2 } ] [ match { internal | external [ 1|2 ] | nssa-external [ 1|2 ] } ] [ metric metric-value ] [ route-map route-map-name ]
```

Parameter Description

Parameter	Description
bgp	Is redistributed from bgp.
connected	Is redistributed from a connected route.
isis <i>area-tag</i>	Is redistributed from ISIS and specifies an ISIS instance through area-tag.
ospf <i>process-id</i>	Is redistributed from OSPF and specifies an OSPF instance through

	process-id. The value is in the range from 1 to 65535.
static	Is redistributed from static routes.
level-1 level-1-2 level-2	Is used when ISIS route redistribution is configured and specifies a route with a specific level for redistribution.
match	Is used when OSPF route redistribution is configured and filters a route with a specific level for redistribution.
metric <i>metric-value</i>	Sets the metric value of the redistributed route and specifies the metric value by using the metric-value parameter. The value is in the range from 1 to 16.
route-map <i>route-map-name</i>	Sets the redistribution filtering rule.

Defaults

By default:

All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF.

The routes of Level-2 sub-types of the instance are redistributed when you configure ISIS redistribution.

All the routes of the protocol are redistributed for other routing protocols.

The metric of the redistributed routes is 1 by default.

The route-map is not associated.

Command**Mode**

Routing process configuration mode

Usage Guide

This command is executed to redistribute external routes to RIP.

It is unnecessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. For RIP, the metric value is calculated based on hop counts; for OSPF, the metric value is calculated based on bandwidths. Therefore, their metrics are not comparable. However, a symbolic metric value must be set for route redistribution. Otherwise, route redistribution will fail.

When you configure ISIS route redistribution without the level parameter, only level-2 routes are redistributed by default. If the redistribution configuration is initialized with the level parameter, then all routes with level configured are redistributed. When the configuration is saved and level 1 and level 2 are configured at the same time, level 1 and level 2 are combined into the level-1-2 parameter to be saved.

When you configure redistribution of OSPF routes without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The no form of this command restores the setting to the default value.

The rule of configuring the no form of the redistribute command is as follows:

1. If the no form of this command specifies certain parameters, the parameters must be restored to the default configuration.
2. If the **no** form of this command does not specify any parameter, the command must be deleted.


Assume that the following configurations are available.

```
redistribute isis 112 level-2
```

You can use the `no redistribute isis 112 level-2` command to modify the configuration. According to the preceding rule, this command only restores the level-2 parameter to the default value. However, level-2 is also the default parameter value. Therefore, the configuration is still be saved as `redistribute isis 112 level-2` after you use the `no` form of this command.

To delete this command, use the following command:

```
no redistribute isis 112
```

 The `redistribute` command cannot redistribute the default route of other protocol to the RIP process. To this end, use the **default-information originate** command.

Configuration The following example redistributes static routes to RIP.

Examples Ruijie(config-router)# redistribute static

**Related
Commands**

Command	Description
default-metric <i>metric</i>	Sets the default metric of the route to be redistributed.
default-information originate	Generates the default route in the RIP process.

Platform N/A

Description

1.34 router rip

Use this command to create the RIP routing process and enter the routing process configuration mode. Use the **no** form of this command to restore the default setting.

router rip

no router rip

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults No RIP process is running by default.

Command

Mode Global configuration mode

Usage Guide One RIP routing process must be defined with one network number. If a dynamic routing protocol runs on asynchronous lines, configure the **async default routing** command on the asynchronous interface.

Configuration Examples The following example creates the RIP routing process and enters the routing process configuration mode.

```
Ruijie (config)# router rip
Ruijie(config-router)#
```

**Related
Commands**

Command	Description
network (RIP)	Defines the network number of the RIP process.

Platform N/A**Description**

1.35 show ip rip

Use this command to display the RIP process information.

show ip rip [vrf vrf-name]

**Parameter
Description**

Parameter	Description
vrf vrf-name	(Optional) Displays the RIP information with the specified VRF.

Defaults N/A**Command****Mode** Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide It is used to display the three timers, routing distribution status, routing re-distribution status, interface RIP version, RIP interface and network range, metric, and distance of the RIP process quickly. If the VRF is specified, the name of VRF and VRF ID are displayed.

Configuration Examples The following example displays the basic information of the RIP process such as the update time and management distance.

```
Ruijie#show ip rip
Routing Protocol is "rip"
  Sending updates every 10 seconds, next due in 4 seconds
  Invalid after 20 seconds, flushed after 10 seconds
  Outgoing update filter list for all interface is: not set
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 2
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface          Send  Recv
  FastEthernet 0/1      2    2
  FastEthernet 0/2      2    2
Routing for Networks:
```

```

192.168.26.0 255.255.255.0
192.168.64.0 255.255.255.0
Distance: (default is 50)

```

The following example specifies the VRF and displays the corresponding basic information of RIP instance.

```

Ruijie(config-router)# sh ip rip vrf 1
VRF 1 VRF-id:1
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 4 seconds
  Invalid after 180 seconds, flushed after 120 seconds
  Outgoing update filter list for all interface is: not set
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 1, receive any version
  Routing for Networks:
  Distance: (default is 120)

```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

1.36 show ip rip database

Use this command to display the route summary information in the RIP routing database.

show ip rip database [*vrf vrf-name*] [*network-number network-mask*] [**count**]

no address-family ipv4 vrf vrf-name

Parameter Description

Parameter	Description
vrf vrf-name	(Optional) Displays the RIP routing information of specified VRF.
<i>network-number</i>	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
<i>network-mask</i>	Indicates the subnet mask. It must be specified if the network number is specified.
count	(Optional) Displays the abstract of the route statistics in the RIP database.

Defaults N/A

Command

Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.

Configuration The following example displays all converged address entries in the RIP routing database.

Examples

```
Ruijie# show ip rip database
192.168.1.0/24    auto-summary
192.168.1.0/30    directly connected, Loopback 3
192.168.1.8/30    directly connected, FastEthernet 0/1
192.168.121.0/24  auto-summary
192.168.121.0/24  redistributed
[1] via 192.168.2.22, FastEthernet 0/2
192.168.122.0/24  auto-summary
192.168.122.0/24
[1] via 192.168.4.22, Serial 0/1 00:28 permanent
```

The following example displays the converged address entries related with 192.168.121.0/24 in the RIP routing database.

```
Ruijie# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24  redistributed
[1] via 192.168.2.22, FastEthernet 0/1
```

The following example displays the statistical information summary of various routes in the RIP routing database.

```
Ruijie# show ip rip database count
           All    Valid  Invalid
database   5      5      0
auto-summary  5      5      0

connected  1      1      0
rip        4      4      0
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently-running routing protocol process.

Platform N/A
Description

1.37 show ip rip external

Use this command to display the information of the external routes redistributed by the RIP protocol.

show ip rip external [bgp | connected | isis [process-id] | ospf process-id | static] [vrf vrf-name]

Parameter Description	Parameter	Description
	bgp	Displays redistributed BGP routes.
	connected	Displays redistributed directly-connected routes.
	isis process-id	Displays redistributed ISIS routes. The process-id parameter indicates ISIS process ID.
	ospf process-id	Displays redistributed OSPF routes. The process-id parameter indicates OSPF process ID. The range is from 1 to 65535.
	static	Displays redistributed static routes.
	vrf vrf-name	Displays the RIP external route of the specified VRF (optional).

Defaults N/A

Command

Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide N/A

Configuration The following example displays direct routes redistributed by the RIP process.

Examples

```
Ruijie# show ip rip external
Protocol connected route:
[connected] 192.100.3.0/24 metric=0
    nhop=0.0.0.0, if=2
[connected] 192.101.1.0/24 metric=0
    nhop=0.0.0.0, if=3
Protocol static route:
[static] 10.1.1.1/32 metric=0
    nhop=0.0.0.0, if=4096
[static] 10.1.2.1/32 metric=0
    nhop=0.0.0.0, if=4096
Protocol ospf 1 route:
[ospf] 1.1.1.1/32 metric=2
    nhop=192.100.3.2, if=2
[ospf] 90.1.1.1/32 metric=2
    nhop=192.100.3.2, if=2
```

Related Commands

Command	Description
---------	-------------

show ip rip	Displays the information of the currently running routing protocol process.
ip vrf	Creates a VRF.

Platform N/A

Description

1.38 show ip rip interface

Use this command to display the RIP interface information.

show ip rip interface [vrf vrf-name] [interface-type interface-number]

Parameter Description	Parameter	Description
	vrf vrf-name	Displays the RIP interface of specified VRF (optional).
	[interface-type interface-number]	Displays the specified interface type and interface number (optional).

Defaults N/A

Command

Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the information about RIP interfaces. If no RIP interface exists, no information is displayed.

Configuration The following example displays the RIP interface information.

Examples

```
Ruijie# show ip rip interface
FastEthernet 0/1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv2 packets only
Send RIPv2 packets only
Recv RIP packet total: 0
Send RIP packet total: 3
Passive interface: Disabled
Split Horizon with Poisoned Reverse: Enabled
Triggered RIP Enabled:
Retransmit-timer: 5, Retransmit-count: 36
V2 Broadcast: Disabled
Multicast registe: Registered
Interface Summary Rip:
Not Configured
Authentication mode: Text
Authentication key-chain: ripk1
```

```

Authentication text-password: ruijie
Default-information: only, metric 5
IP interface address:
192.168.64.100/24, next update due in 14 seconds
2.2.1.1/24, next update due in 24 seconds
    neighbor 2.2.1.6, next update due in 3 seconds
    neighbor 2.2.1.77, next update due in 13 seconds
2.2.2.57/24, next update due in 16 seconds

```

If the BFD has been configured for RIP, the BFD information is also displayed.

```

Ruijie#show ip rip interface
Serial 0/1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 packets only
    Receive RIP packet: Enabled
    Send RIP packet: Enabled
    Send RIP supernet routes: Enabled
    Recv RIP packet total: 0
    Send RIP packet total: 3
    Passive interface: Disabled
Split Horizon: Enabled
Triggered RIP Disabled
  BFD: Enabled
  V2 Broadcast: Disabled
  Multicast registe: Registered
  Interface Summary Rip:
    Not Configured
  IP interface address:
    2.2.2.111/24, next update due in 14 seconds

```

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.

Platform N/A
Description

1.39 show ip rip peer

Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP neighbor information.

```
show ip rip peer [ ip-address ] [ vrf vrf-name ]
```

Parameter Description	Parameter	Description
	<i>ip-address</i>	(Optional) Displays the IP address of a specified RIP neighbor.
	<i>vrf vrf-name</i>	(Optional) Displays the RIP interface of a specified VRF.

Defaults N/A

Command

Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.

Configuration The following example displays the RIP neighbor information.

Examples

```
Ruijie# show ip rip peer
Peer 192.168.3.2:
  Local address: 192.168.3.1
  Input interface: GigabitEthernet 0/2
  Peer version: RIPv1
  Received bad packets: 3
  Received bad routes: 0
  BFD session state up
```

Related Commands	Command	Description
	show ip rip	Displays the information of the routing protocol process that is running.

Platform N/A

Description

1.40 timers basic

Use this command to adjust the RIP clock. Use the **no** form of this command to restore the default setting.

timers basic *update invalid flush*

no timers basic

Parameter Description	Parameter	Description
	<i>update</i>	Indicates the route update time in seconds. The update keyword defines the period at which the device sends route update packets. Each time an update packet is received, the "Invalid" and "Flush"

	clocks are reset. By default, a route update packet is sent every 30 seconds.
<i>invalid</i>	Indicates the route invalid time in seconds, starting from the last valid update packet. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update packet is received within the route invalid period, the related route becomes invalid and enters into the "invalid" state. If an update packet is received within the period, the clock resets. By default, the Invalid time is 180 seconds.
<i>flush</i>	Indicates the route flushing time in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush time is 120 seconds.


Defaults By default, the update time is 30 seconds, the invalid time is 180 seconds, and the flushing time is 120 seconds.

Command

Mode Routing process configuration mode

Usage Guide Adjusting the above clocks may speed up routing protocol convergence and fault recovery. Devices connected to the same network must have consistent RIP clock values. Adjustment of RIP clocks is not recommended unless otherwise specified.

To check the current RIP clock parameters, use the **show ip rip** command.

 If you set the clock to a small value on low-speed links, some risks will be caused because numerous update packets may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2 Mbit/s to reduce the convergence time of routes.

Configuration The following example enables the RIP update packets that are sent every 10 seconds. If no update

Examples packet is received within 30 seconds, related routes become invalid and enter the invalid status.

When another 90s elapses, they will be cleared.

```
Ruijie (config)# router rip
Ruijie (config-router)# timers basic 10 30 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.41 validate-update-source

Use this command to validate the source address of the received RIP route update packet. Use the **no** form of the command to disable this function.

validate-update-source

no validate-update-source

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command

Mode Routing process configuration mode

Usage Guide You can validate the source address of the RIP route update packet. The validation aims to ensure that the RIP routing process receives only the route update packets from the same IP subnet neighbor.

Disabling split horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the

validate-update-source command in routing process configuration mode.

In addition, for the ip unnumbered interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the command **validate-update-source**.

Configuration The following example disables verification of the source IP address of the update packet.

Examples

```
Ruijie (config)# router rip
Ruijie (config-router)# no validate-update-source
```

Related Commands

Command	Description
ip split-horizon	Enables split horizon.
ip unnumbered	Defines the IP unnumbered interface.
neighbor (RIP)	Defines the IP address of a RIP neighbor.

Platform N/A

Description

1.42 version

Use this command to define the RIP version of a device. Use the **no** form of this command to restore the default setting.

version { 1 | 2 }**no version****Parameter
Description**

Parameter	Description
1	Defines the RIP version 1.
2	Defines the RIP version 2.

Defaults

The route update packets of RIPv1 and are received by default, but only the RIPv1 route update packets are sent.

Command**Mode**

Routing process configuration mode

Usage Guide

This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

Configuration

The following example configures the RIP version as version 2.

Examples

```
Ruijie (config)# router rip
Ruijie (config-router)# version 2
```

**Related
Commands**

Command	Description
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
show ip rip	Displays RIP information.

Platform

N/A

Description

2 OSPFv2 Commands

2.1 area

Use this command to configure the specified OSPF area. Use the **no** form of this command to restore the default setting.

area *area-id*

no area *area-id*

Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the OSPF area. The value can be a decimal integer or an IP address.

Defaults No OSPF area is configured by default.

Command

Mode Routing process configuration mode

Usage Guide Use the no form of this command to remove the specified OSPF area and its configuration, including the area-based **area authentication**, **area default-cost**, **area filter-list**, and **area nssa** commands.

- Do not remove the OSPF area configuration under the following conditions:
- Virtual links exist in the backbone area. The virtual links must be removed at first.
- The corresponding network area command exists in any area. All network segment commands added to an area must be removed at first.

Configuration The following example removes the configuration of OSPF area 2.

Examples

```
Ruijie(config)# router ospf 2
Ruijie(config-router)# no area 2
```

Related Commands	Command	Description
	network area	Defines the interface where OSPF runs and the belonging area of the interface.

Platform N/A

Description

2.2 area authentication

Use this command to enable OSPF area authentication. Use the **no** form of this command to restore the default setting.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication**

Parameter Description

Parameter	Description
<i>area-id</i>	Specifies ID of the area enabled with OSPF. The value can be a decimal integer or an IP address.
message-digest	(Optional) Enables MD5 (message digest 5) authentication mode.

Defaults No authentication is enabled by default.

Command

Mode Routing process configuration mode

Usage Guide

The RGOS software supports three authentication types:

1) 0, no authentication. The authentication type in the OSPF packet is 0 when this command is not executed to enable OSPF authentication. 2) 1, plain text authentication mode. When this command is configured, the message-digest option is not used. 3) 2, MD5 authentication mode. When this command is configured, the message-digest option is used.

All devices in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication password must be configured on an interface connecting neighbors. You can use the **ip ospf authentication-key** command to configure the plain text authentication password, and the **ip ospf message-digest-key** command to configure the MD5 authentication password in interface configuration mode.

Configuration Examples The following example uses MD5 authentication and the authentication password backbone in area 0 (backbone area) of the OSPF routing process.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 192.168.12.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 1 md5 backbone
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# area 0 authentication message-digest
```

Related Commands

Command	Description
ip ospf authentication-key	Defines the OSPF plain text authentication password.
ip ospf message-digest-key	Defines the OSPF MD5 authentication password.

area virtual-link	Defines a virtual link.
--------------------------	-------------------------

Platform N/A

Description

2.3 area default-cost

Use this command to define the cost (OSPF metric) of the default aggregate route advertised to the stub area or not-so-stubby area (NSSA) in routing process configuration mode. Use the **no** form of this command to restore the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the stub area or NSSA
<i>cost</i>	Cost of the default aggregate route advertised to the stub area or NSSA. The range is from 0 to 16777215.

Defaults The default is 1.

Command

Mode Routing process configuration mode

Usage Guide This command takes effect only on the Area Border Router (ABR) of the stub area or the ABR/Autonomous System Border Router (ASBR) of the NSSA. The ABR can advertise a Link State Advertisement (LSA) indicating the default route in the stub area. The ABR/ASBR can advertise an LSA indicating the default route in the NSSA. You can use the **area default-cost** command to modify the LSA cost.

Configuration Examples The following example sets the cost of the default aggregate route to 50.

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.255.255 area 0
Ruijie(config-router)#network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area 1 stub
Ruijie(config-router)# area 1 default-cost 50
```

Related Commands

Command	Description
area stub	Sets an OSPF area as a stub area.
area nssa	Sets an OSPF area as an NSSA.

Platform N/A

Description

2.4 area filter-list

Use this command to filter the inter-area routes on the ABR. Use the **no** form of this command to restore the default setting.

area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } { **in** | **out** }

no area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } { **in** | **out** }

Parameter Description

Parameter	Description
<i>area-id</i>	Area ID
<i>acl-name</i>	Name of an Access Control List (ACL)
<i>prefix-name</i>	Prefix-list name
in out	Applies the ACL rule to the routes incoming/outgoing the area.

Defaults No filtering is configured by default.

Command

Mode Routing process configuration mode

Usage Guide This command can be configured only on an ABR.
You can use this command when it is required to filter the inter-area routes on the ABR.

Configuration The following example sets area 1 to learn only the inter-area routes of 172.22.0.0/8.

Examples

```
Ruijie# configure terminal
Ruijie(config)# access-list 1 permit 172.22.0.0 0.255.255.255
Ruijie(config)# router ospf 100
Ruijie(config-router)# area 1 filter-list access 1 in
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

2.5 area nssa

Use this command to set an OSPF area as an NSSA in routing process configuration mode. Use the **no** form of this command to delete the NSSA or the NSSA configuration.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*]

[**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]

```
no area area-id nssa [ no-redistribution ] [ default-information-originate [ metric value ]
[ metric-type type ] ] [ no-summary ] [ translator [ stability-interval | always ] ]
```

**Parameter
Description**

Parameter	Description
<i>area-id</i>	NSSAID
no-redistribution	Imports the routing information to a common area other than the NSSA for the NSSA ABR.
default-information originate	Generates and imports the default Type 7 LSA to the NSSA. This option takes effect only on the NSSA ABR or ASBR.
metric <i>value</i>	Sets the metric of the generated default LSA. The range is from 0 to 16777214. The default value is 1.
metric-type <i>type</i>	Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
no-summary	Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
translator	Configures the translator for the NSSA ABR.
stability-interval <i>seconds</i>	Configures the stability interval in seconds for the NSSA ABR that functions as a translator to change to a non-translator. The range is from 0 to 2147483647. The default value is 40.
always	Configures that an NSSA ABR always functions as a translator. The NSSA ABR is the backup translator by default.

Defaults No NSSA is defined by default.

Command

Mode Routing process configuration mode

Usage Guide The default-information-originate parameter is used to generate the default Type-7 LSA. However, on the NSSA ABR, the default Type-7 LSA will always be generated; On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table.

The no-redistribution parameter prevents the OSPF from advertising the external routes imported with the redistribute command to the NSSA on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR.

To reduce the number of LSAs sent to the NSSA, you can configure the no-summary parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSAs) to the NSSA. In addition, you can use the area default-cost command on the NSSA ABR to configure the cost of the default route advertised to the NSSA. By default, this cost is 1.

If an NSSA has multiple ABRs, the ABR with the greatest ID is selected as the Type-7 or Type-5 translator. To configure that an NSSA ABR always functions as a translator, you can use the translator always parameter. If the translator role of an ABR is taken away by another ABR, the ABR still possesses the conversion capability within stability-interval. If the ABR fails to take back its translator role when stability-interval expires, the LSA that changes from Type-7 to Type-5 will be

removed from the autonomous domain.

To avoid route loops, Type-5 LSAs generated from Type-7 convergence will be eliminated immediately after the current device stopped serving as a translator, with no need to wait until the stability-interval expires.

In a same NSSA, you are recommended to configure the **translator always** parameter on only one ABR.

Configuration The following example sets area 1 as an NSSA on all routers of the area.

Examples

```
Ruijie(config)#router ospf1
Ruijie(config-router)#network 172.16.0.0 0.0.255.255 area0
Ruijie (config-router)#network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area1nssa
```

**Related
Commands**

Command	Description
area default-cost	Defines the cost (OSPF metric) of the default aggregate route advertised to the NSSA.

Platform N/A

Description

2.6 area range

Use this command to configure inter-area route aggregation for OSPF. Use the **no** form of this command to delete route aggregation. Use the **no** form with the cost parameter to restore the default metric of the aggregate route, but not delete route aggregation.

area area-id range ip-address net-mask [advertise | not-advertise] [cost cost]

no area area-id range ip-address net-mask [cost]

**Parameter
Description**

Parameter	Description
<i>area-id</i>	ID of the area where the aggregate route is injected into. The value can be a decimal integer or an IP address.
<i>ip address net-mask</i>	Network segment whose routes are to be aggregated
advertise not-advertise	Whether to advertise the aggregate route
cost cost	Sets the priority of the interface. The range is from 0 to 16777215.

Defaults

No inter-area route aggregation is configured by default.

The configured aggregation range is advertised by default.

The default metric of the aggregate route depends on whether the device is compatible with RFC1583. If yes, the default metric is the smallest cost of the aggregate route. If no, the default metric is the largest cost of the aggregate route.

Command

Routing process configuration mode

Mode

Usage Guide This command takes effect only on the ABR to aggregate multiple routes of an area into a route and advertise it to other areas. Route combination occurs only on the border of an area. The devices inside an area see the specific routing information, but the devices outside the area see only one aggregate route. The advertise and not-advertise options can set whether to advertise the aggregate route for filtering and masking. The aggregate route is advertised by default. You can use the cost option to set the metric of the aggregate route. You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing area. This improves the network forwarding performance, especially in large networks. The area range of route aggregation is determined according to the longest match when multiple aggregate routes with direct inclusion relationships are configured.

Configuration The following example aggregate the routes of area 1 into a route 172.16.16.0/20.

Examples

```
Ruijie(config)#router ospf 1
Ruijie(config-router)#network 172.16.0.0 0.0.15.255area0
Ruijie((config-router)#network 172.16.17.0 0.0.15.255area1
Ruijie(config-router)#area1range 172.16.16.0 255.255.240.0
```

Related Commands

Command	Description
discard-route	Enables a discarded route to be added to a routing table.
summary-address	Configures the OSPF external route aggregation.

Platform N/A

Description

2.7 area stub

Use this command to set an OSPF area as a stub area or full stub area. Use the **no** form of this command to restore the default setting.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter Description

Parameter	Description
<i>area-id</i>	Stub area ID
no-summary	(Optional) Prevents the ABR from advertising the network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.

Defaults No stub area is defined by default.

Command**Mode** Routing process configuration mode

Usage Guide All devices in the OSPF stub area must be configured with the area stub command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. For the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR.

To configure a full stub area, use the area stub command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR.

Two commands can configure an OSPF area as a stub area: the area stub and area default-cost commands. All devices connected to the stub area must be configured with the area stub command, but the area default-cost command can be executed only on the ABR. The area default-cost command defines the initial cost (metric) of the internal default route.

Configuration The following example sets area 1 as the stub area on all devices in area 1.

Examples

```
Ruijie(config)# router ospf1
Ruijie(config-router)# network 172.16.0.0 0.0.255.255 area 0
Ruijie (config-router)# network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area 1 stub
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric value) of the default aggregate route advertised to the stub area.

Platform N/A**Description**

2.8 area virtual-link

Use this command to define the OSPF virtual link in routing process configuration mode. Use the **no** form of this command to restore the default setting.

```
area area-id virtual-link router-id [ authentication [ message-digest | null ] ] [ dead-interval
{ seconds | minimal hello-multiplier multiplier } ] [ hello-interval seconds ] [ retransmit-interval
seconds ] [ transmit-delay seconds ] [ [ authentication-key [ 0|7 ] key ] | [ message-digest-key
key-id md5 [ 0|7 ] key ] ]
```

```
no area area-id virtual-link router-id [ authentication ] [ dead-interval ] [ hello-interval ]
[ retransmit-interval ] [ transmit-delay ] [ [ authentication-key ] | [ message-digest-key key-id ] ]
```

Parameter

Parameter	Description
-----------	-------------

Description	
<i>area-id</i>	ID of the OSPF transition area. The value can be a decimal integer or an IP address.
<i>router-id</i>	ID of the router neighboring to the virtual link. It can be viewed with the show ip ospf command.
dead-interval <i>seconds</i>	(Optional) Defines the time to declare neighbor loss in seconds. The range is 0 to 2147483647. This value must be consistent with that of the neighbor.
minimal	Enables the Fast Hello function and sets the death clock to 1 second.
hello-multiplier	Multiplies dead-interval with hello-interval in the Fast-Hello function.
<i>multiplier</i>	Specifies the number of Hello packets that are sent every second in the Fast Hello function. The range is from 3 to 20.
hello-interval <i>seconds</i>	(Optional) Defines the interval at which the HELLO packet is sent by the OSPF to the virtual link in seconds. The range is from 1 to 65535. This value must be consistent with that of the neighbor.
retransmit-interval <i>seconds</i>	(Optional) OSPF LSA retransmission interval in seconds. The range is from 0 to 65535. The parameter setting must consider the round-trip time of packets on the link.
transmit-delay <i>seconds</i>	(Optional) OSPF LSA transmission delay in seconds. The range is from 0 to 65535. This value adds the LSA keep alive period. When the LSA keep alive period reaches a threshold, the LSA will be refreshed.
authentication-key [0 7] <i>key</i>	(Optional) Defines the OSPF plain text authentication key. The plain text authentication key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
message-digest-key <i>key-id</i> md5 [0 7] <i>key</i>	(Optional) Defines the OSPF MD5 authentication key and key ID. The MD5 authentication key ID and key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
authentication	Sets the authentication type to plain text.
message-digest	Sets the authentication type to MD5.
null	Sets the authentication type to no authentication.

Defaults

The following are the default values:

dead-interval: 40seconds

hello-interval: 10seconds

retransmit-interval: 5seconds

transmit-delay: 1second

authentication: null

The Fast Hello function is disabled by default.
The other parameters do not have default values.

Command

Mode Routing process configuration mode

Usage Guide

A virtual link can connect an area to the backbone area, or another non-backbone area. In the OSPF routing domain, all areas must connect to the backbone area. If an area disconnects from the backbone area, a virtual link to the backbone area is required. Otherwise, the network communication will become abnormal. The virtual link is created between two ABRs. The area that belongs to both ABRs is called the transition area, which can never be a stub area or NSSA.

The router-id parameter indicates the ID of OSPF neighbor router and can be displayed with the show ip ospf neighbor command. You can configure the loopback address as the router ID.

The area virtual-link command defines only the authentication key for a virtual link. You can use the area authentication command to enable the OSPF packet authentication in areas connected over the virtual link in routing process configuration mode.

OSPF supports the Fast Hello function.

If the Fast Hello function is enabled, the OSPF can discover neighbors and detects invalid neighbors quickly. You can enable the OSPF Fast Hello function by specifying the keywords minimal and hello-multiplier, and the multiplier parameter. You can set the death clock to 1 second in minimal and hello-multiplier to a value equal to or greater than 2. In this case, the Hello packet sending interval is less than 1 second.

The hello-interval field of a Hello packet received by a virtual link is omitted if the Fast Hello function is enabled on the virtual link and the hello-interval field is set to 0 for Hello packets advertised from the virtual link.

No matter the Fast Hello function is enabled or not, the values of dead-interval must be consistent on both ends of a virtual link. The values of hello-multiplier on both ends can be different if at least one Hello packet can be received within dead-interval. You can use the show ip ospf virtual-links command to monitor dead-interval and hello-interval configured for a virtual link.

For the Fast Hello function, you can only configure either the **dead-interval minimal hello-multiplier** parameter or the **hello-interval** parameter.

Configuration

The following example sets area 1 as the transition area to establish virtual link with neighbor 2.2.2.2.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.15.255 area0
Ruijie(config-router)# network 172.16.17.0 0.0.15.255 area1
Ruijie(config-router)#area1 virtual-link2.2.2.2
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1. This virtual link connects area 10 and the backbone area, and works with the OSPF packet authentication in MD5 mode.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.17.0 0.0.15.255area1
Ruijie(config-router)# network172.16.252.0 0.0.0.255 area10
```



```
Ruijie(config-router)# area 0 authentication message-digest
Ruijie(config-router)# area1virtual-link 1.1.1.1message-digest-key1md5hello
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1, enables the Fast Hello function on this virtual link, and sets the multiplier to 3.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.17.0 0.0.15.255 area1
Ruijie(config-router)# network 172.16.252.0 0.0.0.255 area10
Ruijie(config-router)# area1 virtual-link1.1.1.1dead-interval minimal
hello-multiplier 3
```

Related Commands

Command	Description
area authentication	Enables the OSPF area packet authentication and define the authentication mode.
show ip ospf	Displays the OSPF process information, including the router ID.
show ip ospf virtual-links	Monitors information about a virtual link.

Platform N/A

Description

2.9 auto-cost

Use this command to enable the auto-cost function and set the reference bandwidth according to the reference bandwidth. Use the **no** form of this command to restore the default setting.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
<i>ref-bw</i>	Reference bandwidth, in the range from 1 to 4294967 Mbps.

Defaults The default is 100Mbps.

Command

Mode Routing process configuration mode

Usage Guide

By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth.

Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps.

Run the **bandwidth** command to set the interface bandwidth.

The costs of OSPF interfaces on several typical lines are as follows:

64Kbps serial line: The cost is 1562.

E1 line: The cost is 48.

10M Ethernet: The cost is 10.

100M Ethernet: The cost is 1.

If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration The following example configures the reference bandwidth as 10 Mbps.

Examples

```
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.10.0 0.0.0.255 area0
Ruijie(config-router)# auto-costreference-bandwidth10
```

**Related
Commands**

Command	Description
show ip ospf	Displays the OSPF global configuration information
ip ospf cost	Sets the cost value of the OSPF interface.
bandwidth	Sets the interface bandwidth. This setting does not affect data transmission rate.

Platform N/A

Description

2.10 bfd all-interfaces

Use this command to enable Bidirectional Forwarding Detection (BFD) on all OSPF interfaces. Use the **no** form of this command to restore the default setting.

bfd all-interfaces

no bfd all-interfaces

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults BDF is disabled by default.

Command

Mode Routing process configuration mode

Usage Guide OSPF dynamically discovers the neighbors through Hello packets. With the BFD function enabled, one BFD session will be established for the neighbors that match the FULL rules and the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPF will converge with the network immediately.

You can also use the **ip ospf bfd [disable]** command in interface configuration mode to enable or disable the BFD function on the specified interface, which takes precedence over the **bfd**

all-interfaces command in routing process configuration mode.

Configuration Ruijie(config)# router ospf 1
Examples Ruijie(config-router)# bfd all-interfaces

Related Commands	Command	Description
	router ospf	Creates the OSPF routing process and enters routing process configuration mode.
ip ospf bfd]	Enables the specified interface running OSPF or disabling BFD for link detection.	

Platform N/A
Description

2.11 capability opaque

Use this command to enable Opaque LSA. Use the **no** form of this command to disable this function.

capability opaque

no capability opaque

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Opaque LSA is enabled by default.

Command Mode Routing process configuration mode.

Usage Guide N/A

Configuration The following example disables Opaque LSA capability.

Examples Ruijie(config)# router ospf 1
Ruijie(config-router)# no capability opaque

Related Commands	Command	Description
	show ip ospf	Displays the global configuration of OSPF.

Platform N/A
Description

2.12 clear ip ospf process

Use this command to clear and restart the OSPF instance.

clear ip ospf (*process-id*) process

Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF instance ID. When the ID is specified, the command clears data related to the specified instance and restarts the OSPF instance. When no ID is specified, the command clears data related to all running OSPF instances and restarts all the running OSPF instances.

Defaults The rule recommended in the RFC 1583 is used by default.

Command

Mode Privileged EXEC mode

Usage Guide Resetting the entire OSPF process causes that all neighbors are re-established and OSPF is greatly affected. Therefore, you are prompted to confirm the execution for deliberation.

Configuration The following example clears data of OSPF instance 1 and restarts OSPF instance 1.

Examples Ruijie#clearipospflprocess

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.13 compatible rfc1583

Use this command to determine the RFC 1583 or RFC 2328 rule for selecting the optimal route among route table several routes to the same destination out of the Autonomous System (AS).

compatible rfc1583

no compatible rfc1583

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The RFC 1583 rule is used by default.

Command**Mode** Routing process configuration mode**Usage Guide** N/A**Configuration** The following example determines the best route with the RFC 2328 rule.**Examples**

```
Ruijie(config)# routerospf1
Ruijie(config-router)# nocompatibleRFC1583
```

**Related
Commands**

Command	Description
show ip ospf	Displays the OSPF global configuration information

Platform N/A**Description**

2.14 default-information originate

Use this command to generate a default route to be injected into the OSPF routing domain in routing process configuration mode. Use the **no** form of this command to restore the default setting.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

**Parameter
Description**

Parameter	Description
always	(Optional) Generates the default route unconditionally, no matter whether the default route exists locally or not.
metric <i>metric</i>	(Optional) Initial metric of the default route in the range from 0 to 16777214
metric-type <i>type</i>	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics on different devices; type 2, same metric on different devices. An external route of type 1 is more trustworthy than that of type 2.
route-map <i>map-name</i>	Associated route map name. No route map is associated by default.

Defaults No default route is generated by default.
The default value of metric is 1.
The default value of metric-type is 2.

Command Routing process configuration mode

Mode


Usage Guide When the **redistribute** or **default-information** command is executed, the OSPF-enabled device automatically turns into the ASBR. The ASBR cannot generate the default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR can generate the default route with the **default-information originate** command in routing process configuration mode. If the **always** parameter is used, the OSPF routing process advertises an external default route to neighbors, no matter the default route exists or not. However, the local device does not display the default route. To make sure whether the default route is generated, use the **show ip ospf database** command to display the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. You can use the **show ip route** command on the OSPF neighbor to display the default route.

The metric of the external default route can be defined only with the **default-information originate** command.

There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, the type 1 route takes precedence over the type 2 route. As a result, the **show ip route** command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area. To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

 The range of set metric is 0 to 16777214 for the associated route map. If the value exceeds the range, introducing a route fails.

Configuration Examples The following example configures that OSPF generates an external default route and injects it to the OSPF routing domain. The default route is of type 1 and the metric 50.

```
Ruijie(config)#routerospf 1
Ruijie(config-router)#network172.16.24.0 0.0.0.255 area 0
Ruijie(config-router)#default-information originate
alwaysmetric50metric-type1
```

Related Commands

Command	Description
show ip ospf database	Displays OSPF link state database.
show ip route	Displays the IP route table.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

2.15 default-metric

Use this command to set the **default metric** of OSPF redistribution route. Use the **no** form of this command to restore the default setting.

default-metric *metric*

no default-metric

Parameter Description	Parameter	Description
	<i>metric</i>	Default metric of the OSPF redistribution route in the range from 1 to 16777214

Defaults The default metric is not configured by default.

Command

Mode Routing process configuration mode

Usage Guide The **default-metric** command must work with the **redistribute** command in routing process configuration mode to modify the initial metric of all redistributed routes. The configuration result of the **default-metric** command does not take effect for the external routes injected into the OSPF routing domain with the **default-information originate** command.

Configuration The following example configures the default metric of the OSPF redistribution route as 50.

Examples

```
Switch(config)# router rip
Ruijie(config-router)# network 192.168.12.0
Switch(config-router)# version 2
Ruijie(config-router)# exit
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.10.0 0.0.0.255 area 0
Switch(config-router)# default-metric 50
Ruijie(config-router)# redistribute rip subnets
```

Related Commands	Command	Description
	redistribute	Redistributes the routes of other routing processes.
	show ip ospf	Displays the OSPF global configuration information.

Platform N/A

Description

2.16 discard-route

Use this command to enable adding the discard-route into the core route table. Use the **no** form of this command to disable this function.

discard-route { **internal** | **external** }

no discard-route { **internal** | **external** }

Parameter Description	Parameter	Description
	internal	Enables adding the discard-route generated with the area range command
	external	Enables adding the discard-route generated with the summary-address command.

Defaults Adding the discard-route is enabled by default.

Command

Mode Routing process configuration mode

Usage Guide After route aggregation, the range may exceed the actual network range of the route table, and sending the data to the nonexistent network may cause loops or increase router loads. To prevent this situation, the discard-route is added to the route table on the ABR or the ASBR. The discard-route is generated automatically and will not be transmitted.

Configuration The following example disables adding the discard routes generated with the area range command.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no discard-route internal
```

Related Commands

Command	Description
area range	Configures the route aggregation between OSPF areas.
summary-address	Configures the route aggregation out of the OSPF routing domain.

Platform N/A

Description

2.17 distance ospf

Use this command to set the Administration Distance (AD) of different types of OSPF routes. Use the **no** form of this command to restore the default setting.

distance { *distance* | **ospf** { [*intra-area distance*] [*inter-area distance*] [*external distance*] } }

no distance [ospf]**Parameter
Description**

Parameter	Description
<i>distance</i>	Sets the route AD in the range from 1 to 255.
intra-area <i>distance</i>	Sets the AD of the intra-area route in the range from 1 to 255.
inter-area <i>distance</i>	Sets the AD of the inter-area route in the range from 1 to 255.
External <i>distance</i>	Sets the AD of the external route in the range from 1 to 255.

Defaults

The default value is 110.
 The default intra-area distance is 110.
 The default inter-area distance is 110.
 The default external distance is 110.

Command**Mode**

OSPF Routing process configuration mode

Usage Guide

This command is used to specify different ADs for different types of OSPF routes.

Configuration

The following example sets the OSPF external route AD to 160.

Examples

```
Ruijie(config)# routerospf1
Ruijie(config-router)# distance ospf external 160
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

2.18 distribute-list in

Use this command to configure LSA filtering. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | *prefix prefix-list-name* [**gateway** *prefix-list-name*] |

route-map *route-map-name* } *in* [*interface-type interface-number*]

no distribute-list { [*access-list-number* | *name*] | *prefix prefix-list-name* [**gateway** *prefix-list-name*] |

route-map *route-map-name* } *in* [*interface-type interface-number*]

**Parameter
Description**

Parameter	Description
<i>access-list-number</i> name	Uses the ACL filtering rule.
gateway <i>prefix-list-name</i>	Uses the gateway filtering rule.

Prefix <i>prefix-list-name</i>	Uses the prefix-list filtering rule.
route-map <i>route-map-name</i>	Uses the route-map filtering rule.
<i>interface-type</i> <i>interface-number</i>	Configures the LSA route filtering on the interface.

Defaults No filtering is configured by default.

Command

Mode Routing process configuration mode

Usage Guide This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the Shortest Path First (SPF) calculation to generate the corresponding routes. It does not affect the link status database or the route table of the neighbors. It only affects the routing entries calculated by local OSPF. This function is used to control routes that enter the ABR or ASBR.

The following route-map rules will be supported if the route-map parameter is configured:

match interface

match ip address

match ip address prefix-list

match ip next-hop

match ip next-hop prefix-list

match metric

match route-type

match tag

Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration The following example configures LSA filtering.

```
Ruijie(config)# access-list 3 permit 172.16.0.0 0.0.127.255
Ruijie(config)# router ospf 25
Ruijie(config-router)# distribute-list 3 in ethernet 0/1
```

**Related
Commands**

Command	Description
distribute-list out	Filters redistribution routes.

Platform N/A
Description

2.19 distribute-list out

Use this command to configure filtering redistribution routes. The function is similar to that of the **redistribute** command. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

Parameter Description	Parameter	Description
	<i>access-list-number</i> <i>name</i>	Uses the ACL filtering rule.
	prefix <i>prefix-list-name</i>	Uses the prefix-list filtering rule.
	bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static	Source of the routes to be filtered

Defaults No filtering is configured by default.

Command

Mode Routing process configuration mode

Usage Guide Similar to the redistribute route-map command, the distribute-list out command filters the routes that other protocols redistribute to the OSPF. However, the distribute-list out command does not redistribute routes by itself. It works with the redistribute command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration, that is, the two rules cannot be configured at the same time for routes from the same source.

Configuration The following example filters the redistributed static routes.

Examples

```
Ruijie(config)# routerospf1
Ruijie(config)# redistribute static subnets
Ruijie(config-router)# distribute-list 22 outstatic
Ruijie(config-router)# distribute-list prefix jjj out static
% Access-list filter exists, please de-config first
```

Related Commands

Command	Description
distribute-list in	Configures LSA filtering.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

2.20 enable mib-binding

Use this command to bind the Management Information Base (MIB) with the specified OSPFv2 process. Use the **no** form of this command to restore the default setting.

enable mib-binding

no enable mib-binding

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The MIB is bound with the OSPFv2 process with the smallest ID by default.

Command

Mode Routing process configuration mode

Usage Guide OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is bound with the OSPFv2 process with the smallest ID. User operations take effect for this process.

To operate the specified OSPF process over Simple Network Management Protocol(SNMP), use this command to bind the MIB to SNMP.

Configuration The following example operates OSPFv2 process 100 over SNMP:

Examples

```
Ruijie(config)# routerospf100
Ruijie(config-router)# enable mib-binding
```

Related Commands	Command	Description
	show ip ospf	Displays the OSPF global configuration information.
	enable traps	Configures the OSPF TRAP function.

Platform N/A

Description

2.21 enable traps

The OSPFv2 process supports 16 kinds of TRAP packets, which are classified into four categories. Use this command to enable sending the specified TRAP messages. Use the **no** form of this command to restore the default setting.

enable traps [error [IfAuthFailure | IfConfigError | IfRxBadPacket | VrtIfAuthFailure | VrtIfConfigError | VrtIfRxBadPacket]] | lsa [LsdbApproachOverflow | LsdbOverflow | MaxAgeLsa | OriginateLsa]] | retransmit [IfTxRetransmit | VrtIfTxRetransmit]] | state-change

```
[ IfStateChange | NbrRestartHelperStatusChange | NbrStateChange |
NssaTranslatorStatusChange | RestartStatusChange | VirtIfStateChange |
VirtNbrRestartHelperStatusChange | VirtNbrStateChange ] ]
no enable traps [ error [ IfAuthFailure | IfConfigError | IfRxBadPacket | VirtIfAuthFailure |
VirtIfConfigError | VirtIfRxBadPacket ] | Isa [ LsdbApproachOverflow | LsdbOverflow |
MaxAgeLsa | OriginateLsa ] | retransmit [ IfTxRetransmit | VirtIfTxRetransmit ] | state-change
[ IfStateChange | NbrRestartHelperStatusChange | NbrStateChange |
NssaTranslatorStatusChange | RestartStatusChange | VirtIfStateChange |
VirtNbrRestartHelperStatusChange | VirtNbrStateChange ] ]
```

**Parameter
Description**

Parameter	Description
error	Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches.
	Ifauthfailure Interface authentication error
	Ifconfigerror Interface parameter configuration error
	Ifrxbadpacket Error packets received on the interface
	Virtifauthfailure Authentication error on the virtual interface
	Virtifconfigerror Parameter configuration error on the virtual interface
isa	Configures all traps switches related to the LSA. Use this parameter to set the following specified LSA traps switches.
	Lsdbapproachoverflow External LSA count has reached the 90% of the upper limit.
	Lsdboverflow External LSA count has reached the upper limit.
	Maxagelsa LSA reaching the aging time
	Originatelsa Generates new LSA
retransmit	Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches.
	Iftxretransmit Packet retransmission on the interface
	Virtiftxretransmit Packet retransmission on the virtual interface
state-change	Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches.
	Ifstatechange Interface state change
	NbrRestartHelperStatusChange State change during the neighbor GR process
	Nbrstatechange Neighbor state change
	NssaTranslatorStatusChange State change of the NSSA translator
	RestartStatusChange State change of the GR Restarter on the device

	Virtifstatechange	State change on the virtual interface
	VirtNbrRestartHelper StatusChange	Status change of the virtual neighbor GR process
	Virtnbrstatechange	State change on the virtual neighbor

Defaults All TRAP switches are disabled by default.

Command

Mode Routing process configuration mode

Usage Guide The **snmp-server enable traps ospf** command must be configured before you configure this command, for it is limited by the **snmp-server** command.
This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Configuration The following example enables all TRAP switches of OSPFv2 process 100.

```
Ruijie(config)# routerospf100
Ruijie(config-router)# enable traps
```

**Related
Commands**

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable mib-binding	Binds the OSPFv2 process with MIB.
snmp-server enable traps ospf	Enables the OSPF TRAP notification function.

Platform N/A

Description

2.22 fast-reroute

Use this command to enable the OSPF FRR (Fast Reroute) function for the device. Use the **no** form of this command to restore the default setting.

```
fast-reroute { lfa | downstream-paths | route-map route-map-name }
no fast-reroute { lfa [ downstream-paths ] | route-map }
```

**Parameter
Description**

Parameter	Description
lfa	Enables the LFA (loop-free alternate) path computation.
downstream-paths	Enables the downstream path computation.
route-map route-map-name	Specifies the backup path through the route map.

Defaults	The FRR function is disabled by default.
Command	
Mode	Routing process configuration mode
Usage Guide	<p>If the ifa parameter is configured, computation of the loop-free standby path is enabled. In this case, you can use the interface mode command to specify the path protection mode of the interface. It is recommended that computation of the loop-free standby path be disabled if any of the following case exists on the network:</p> <ol style="list-style-type: none"> 1. Virtual links exist. 2. Alternative ABRs exist. 3. An ASBR is also an ABR. 4. Multiple ABSRs advertise the same external route. <p>If both ifa and downstream-paths are configured, computation of the downstream path is enabled. If route-map is configured, a standby path can be specified for a matched route through the route-map.</p> <p>When the OSPF fast reroute function is used, it is recommended that BFD be enabled at the same time so that the device can quickly detect any link failure and therefore shorten the forwarding interruption time. If the interface is up or down, to shorten the forwarding interruption time during OSPF fast reroute, you can configure carrier-delay 0 in L3 interface configuration mode to achieve the fastest switchover speed.</p>

Configuration The following example enables FRR for OSPF instance 1 and associates route map *fast reroute*.

```
Ruijie(config)# route-map fast-reroute
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set fast-reroute backup-next-hop GigabitEthernet 0/1
192.168.1.2
Ruijie(config)# router ospf 1
Ruijie(config-router)# fast-reroute route-map fast-reroute
```

Related Commands	Command	Description
	graceful-restart helper	Enables the OSPF graceful-restart helper.

Platform N/A
Description

2.23 graceful-restart

Use this command to enable the graceful restart (GR) of OSPF on the device. Use the **graceful-restart grace-period** command to configure the grace period parameter and enable the OSPF GR function. Use the **no** form of this command to disable this function.

graceful-restart [grace-period *grace-period* | inconsistent-lsa-checking]

no graceful-restart [graceful-period]

Parameter Description	Parameter	Description
	grace-period <i>grace-period</i>	Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is 120s.
	inconsistent-lsa-checking	Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence. After GR is enabled, topological change detection is enabled by default.

Defaults This function is enabled by default.

Command

Mode Routing process configuration mode

Usage Guide GR is configured based on the OSPF instance. Different instances could be configured with different parameters according to the actual situation.

The graceful restart interval is the longest time between the OSPF restart and the graceful restart. In this period, you can perform link status reconstruction to restore the OSPF status to the original. With the interval times out, the OSPF will exit GR and perform common OSPF operations.

The GR interval is 120 seconds set with the graceful-restart command, and the graceful-restart grace-period command allows you to change the interval explicitly.

GR is unavailable when the Fast Hello function is enabled.

Configuration The following example enables GR for the OSPF instance 1 and sets the restart interval for GR.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# graceful-restart
Ruijie(config-router)# graceful-restart grace-period 60
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPF graceful-restart helper.

Platform N/A

Description

2.24 graceful-restart helper

Use this command to enable the graceful restart helper function. Use the **no** form of this command to restore the default setting.

graceful-restart helper disable

no graceful-restart helper disable

graceful-restart helper { **strict-lsa-checking** | **internal-lsa-checking** }
no graceful-restart helper { **strict-lsa-checking** | **internal-lsa-checking** }

**Parameter
Description**

Parameter	Description
disable	Prohibits a device from acting as a GR helper for another device.
strict-lsa-checking	Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
internal-lsa-checking	Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.

Defaults

The GR helper is enabled by default.

The router enabled with the GR helper does not check the LSA change by default.

Command

Mode

Routing process configuration mode

Usage Guide

This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR.

After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (**strict-lsa-checking** and **internal-lsa-checking**) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration

The following example disables the GF helper and modifies the policy of checking network changes.

Examples

```
Ruijie(config)# router ospf1
Ruijie(config-router)# graceful-restart helper disable
Ruijie(config-router)# no graceful-restart helper disable
Ruijie(config-router)# graceful-restart helper
strict-lsa-checking
```

Related

Commands

Command	Description
---------	-------------

graceful-restart	Enables GR on the device.
-------------------------	---------------------------

Platform N/A

Description

2.25 ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of this command to restore the default setting.

ip ospf authentication [message-digest | null]

no ip ospf authentication

Parameter	Parameter	Description
Description	message-digest	Enables MD5 authentication on the interface.
	null	Enables no authentication.

Defaults No authentication mode is configured and that of the local area is used on the interface by default.

Command

Mode Interface configuration mode

Usage Guide Plaintext authentication is applicable when **no** option is used with the command. Note that the no form of this command restores the default value. Whether authentication is used actually depends on authentication mode configured for the local area of the interface. If authentication mode is configured as **null**, no authentication is enabled. When both the interface and its area are configured with authentication, the one for the interface takes precedence.

Configuration The following example configures MD5 authentication for OSPF on fastEthernet 0/1.

Examples

```
Ruijie (config)#interface fastEthernet0/1
Ruijie(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication
message-digest
```

Related Commands	Command	Description
	area authentication	Enables authentication and defines authentication mode in the OSPF area.
	ip ospf authentication-key	Configures the plain text authentication key.
	ip ospf message-digest-key	Configures the MD5 authentication key.

Platform N/A

Description

2.26 ip ospf authentication-key

Use this command to configure the OSPF plain text authentication key in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf authentication-key [0 | 7] *key*

no ip ospf authentication-key

Parameter Description

Parameter	Description
0	Displays the key in plain text.
7	Displays the key in cipher text.
<i>key</i>	Key containing at most eight characters.

Defaults It is disabled by default.

Command

Mode Interface configuration mode

Usage Guide The **ip ospf authentication-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys may vary by interface, but the devices that are connected to the same physical network segment must use the same key.

To enable the OSPF area authentication, execute the area authentication command in routing process configuration mode.

The authentication can be enabled separately on an interface by executing the ip ospf authentication command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

Configuration Examples The following example configures the OSPF authentication key ospfauth for fast Ethernet 0/1.

Examples

```
Ruijie (config)#interfacefastEthernet0/1
Ruijie(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode
ip ospf authentication	Enables authentication on the interface and defines authentication mode

Platform N/A

Description

2.27 ip ospf bfd

Use this command to enable or disable the BFD on the specified OSPF interface. Use the **no** form of this command to restore the default setting.

ip ospf bfd [disable]

no ip ospf bfd [disable]

Parameter Description	Parameter	Description
	disable	Disables BFD on the specified OSPF interface.

Defaults BFD is not configured by default, and the BFD configuration in OSPF process configuration mode shall prevail.

Command

Mode Interface configuration mode

Usage Guide The interface-based configuration takes precedence over the **bfd all-interfaces** command used in process configuration mode.

Based on the actual environment, you can run the **ip ospf bfd** command to enable BFD on a specified interface for link detection, or run the **bfd all-interfaces** command in OSPF process configuration mode to enable BFD on all interface of the OSPF process, or run the **ospf bfd disable** command to disable BFD on a specified interface.

Configuration Ruijie(config)# interface fastethernet 0/1

Examples Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0

Ruijie(config-if-FastEthernet 0/1)# ip ospf bfd

Related Commands	Command	Description
	router ospf	Creates the OSPF routing process and enters routing process configuration mode.
	bfd all-interfaces	Enables the BFD on all OSPF interfaces.

Platform N/A

Description

2.28 ip ospf cost

Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf cost *cost*

no ip ospf cost

**Parameter
Description**

Parameter	Description
<i>cost</i>	OSPF interface cost in the range from 0 to 65535

Defaults

The default interface cost is calculated as follows:

Reference bandwidth/Bandwidth

The reference bandwidth is 100 Mbps by default.

Command

Mode

Interface configuration mode

Usage Guide

By default, the OSPF interface cost is 100Mbps/Bandwidth, where Bandwidth is the interface bandwidth configured with the bandwidth command in interface configuration mode.

The default costs of different types of lines are as follows:

- 64K serial line: 1562
- E1 line: 48
- 10M Ethernet: 10
- 100M Ethernet: 1

The OSPF cost configured with the **ip ospf cost** command will overwrite the default configuration.

Configuration

The following example configures the OSPF cost of fastEthernet 0/1 to 100.

Examples

```
Ruijie(config)# interfacefastEthernet0/1
Ruijie(config-if-FastEthernet 0/1)# ipospfcost100
```

**Related
Commands**

Command	Description
bandwidth	Specifies the interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Displays the OSPF global configuration information

Platform

N/A

Description

2.29 ip ospf database-filter all out

Use this command to stop advertising LSAs of an interface, that is, the LSA update packets are not sent on the interface. Use the **no** form of the command to restore the default setting.

ip ospf database-filter all out

no ip ospf database-filter**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is disabled and all LSA update packets can be sent on the interface by default.

Command

Mode Interface configuration mode

Usage Guide To stop sending LSA update packets on the interface, enable this function on the interface. Then, the device maintains the neighboring connections and accepts LSAs from neighbors, but stops sending LSAs to neighbors.

Configuration The following example stops sending LSA update packets of fastEthernet 0/1.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf database-filter all out
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

2.30 ip ospf dead-interval

Use this command to configure the interval for determining the death of an interface neighbor in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf dead-interval { *seconds* | **minimal** **hello-multiplier** *multiplier* }

no ip ospf dead-interval

**Parameter
Description**

Parameter	Description
<i>seconds</i>	Defines the interval for determining the neighbor death in seconds. The range is from 0 to 2,147,483,647.
minimal	Indicates that the Fast Hello function is enabled to set the dead interval to 1s.
hello-multiplier <i>multiplier</i>	Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20.

Defaults The value of dead-interval is 4 times the interval configured with the **ip ospf hello-interval** command

by default.

Command

Mode Interface configuration mode

Usage Guide

The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically.

When using this command to manually modify the dead interval, pay attention to the following issues:

1. The dead interval cannot be shorter than the Hello interval.
2. The dead interval must be the same on all routers in the same network segment.

OSPF supports the Fast Hello function.

After the OSPF Fast Hello function is enabled, OSPF finds neighbors and detects neighbor failures faster. You can enable the OSPF Fast Hello function by specifying the **minimal** and **hello-multiplier** keywords and the **multiplier** parameter. The **minimal** keyword indicates that the death interval is set to 1s, and **hello-multiplier** indicates the number of Hello packets sent per second. In this way, the interval at which the Hello packet is sent decreases to less than 1s.

If the Fast Hello function is configured for a virtual link, the Hello interval field of the Hello packet advertised on the virtual link is set to 0, and the Hello interval field of the Hello packet received on this virtual link is ignored.

No matter whether the Fast Hello function is enabled, the death interval must be consistent and the **hello-multiplier** values can be inconsistent on routers at both ends of the virtual link. Ensure that at least one Hello packet can be received within the death interval.

Run the **show ip ospf virtual-links** command to monitor the death interval and Fast Hello interval configured for the virtual link.

The **dead-interval minimal hello-multiplier** and **hello-interval** parameters introduced for the Fast Hello function cannot be configured simultaneously.

Configuration

The following example configures the interval for determining the death of the OSPF neighbor on fastEthernet 0/1 to 30 seconds.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf dead-interval 30
```

The following example configures the value of hello-multiplier to 3.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf dead-interval minimal hello-multiplier 3
```

Related

Commands

Command	Description
---------	-------------

ip ospf hello-interval	Specifies the interval at which the OSPF sends Hello packets
show ip ospf interface	Displays OSPF interface information.

Platform N/A

Description

2.31 ip ospf disable all

Use this command to prevent the specified interface from generating OSPF packets. Use the **no** form of this command to restore the default setting.

ip ospf disable all

no ip ospf disable all

Parameter Description	Parameter	Description
	N/A	N/A

Defaults OSPF packets are generated on the specified interface by default.

Command

Mode Interface configuration mode

Usage Guide The interface configured with this command will ignore whether the network areas are matched. After this command is configured, an interface will not generate OSPF packets even if the interface belongs to the network; therefore, the interface does not receive or send any OSPF packets or participate in OSPF calculation.

Configuration The following example prevents the specified interface from generating OSPF packets.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf disable all
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.32 ip ospf fast-reroute no-eligible-backup

Use this command in interface configuration mode to exclude an OSPF interface as a backup

interface in OSPF fast reroute calculation. Use the **no** form of this command to restore the default setting.

ip ospf fast-reroute no-eligible-backup
no ip ospf fast-reroute no-eligible-backup

Parameter Description	Parameter	Description
	N/A	N/A

Defaults An OSPF interface can serve as a backup interface by default.

Command

Mode Interface configuration mode

Usage Guide If the remaining bandwidth of an interface is small or if the interface and its active interface may fail at the same time, the interface cannot be used as a standby interface. Therefore, you need to run this command in interface configuration mode to prevent this interface from becoming a standby interface during OSPF fast reroute computation. After this command is executed, the standby interface is selected from other interface.

This command does not take effect if **fast-reroute route-map** is configured.

Configuration Examples The following example excludes FastEthernet 0/1 as a backup interface in OSPF fast reroute calculation.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf fast-reroute no-eligible-backup
```

Related Commands

Command	Description
fast-reroute	Enables OSPF fast reroute.

Platform Description

N/A

2.33 ip ospf fast-reroute protection

Use this command to specify the loop-free alternate (LFA) protection mode for an interface. Use the **no** form of this command to restore the default setting.

ip ospf fast-reroute protection { node | link-node | disable }
no ip ospf fast-reroute protection

Parameter Description	Parameter	Description
	node	Enables LFA node protection.

link-node	Enables LFA link node protection.
disable	Disables LFA protection.

Defaults LFA node protection is enabled by default.

Command

Mode Interface configuration mode

Usage Guide Enabling the **fast-reroute lfa** command in OSPF process configuration mode will enable OSPF fast reroute and generate a backup route for the master route according to the specified LFA protection mode in interface configuration mode. By default, link protection is enabled on each OSPF interface. In this protection mode, the failure of a master link does not affect forwarding on the backup route. Use the **node** parameter to enable node protection for an interface, that is, the neighbor node of a master link does not affect forwarding on the backup route. Similarly, use the **link-node** parameter to protect the link and neighbor link of a master route at the same time. Use the **disable** parameter to disable the LFA protection function for an interface, that is, a backup entry is not generated for the routes with this interface as the next hop.

Configuration The following example sets OSPF LFA fast reroute to link and node protection:

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf fast-reroute protection link-node
```

Related Commands	Command	Description
	fast-reroute	Enables OSPF fast reroute.

Platform N/A
Description

2.34 ip ospf hello-interval

Use this command to set the interval for sending Hello packets in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf hello-interval *seconds*
no ip ospf hello-interval

Parameter Description	Parameter	Description
	<i>seconds</i>	Interval for sending Hello packets in seconds. The range is from 1 to 65535.

Defaults The defaults are as follows:

10seconds for Ethernet
 10seconds for PPP or HDLC encapsulated interfaces
 10seconds for frame relay PTP interfaces
 30seconds for non-frame relay PTP sub-interface and X.25 interfaces

Command

Mode Interface configuration mode

Usage Guide The interval of sending the Hello packets is included in the Hello packet. A shorter interval means that OSPF detects the topological change faster, which will increase network traffic. The Hello packet sending intervals for all the devices in the same network segment must be the same. To manually modify the interval to determine neighbor death, ensure that the Hello packet sending interval cannot be greater than dead-interval of the neighbor.

Configuration The following example configures the interval of sending the Hello packets on fastEthernet 0/1 to15.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf hello-interval 15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the interval for determining the death of the OSPF neighbor.

Platform N/A

Description

2.35 ip ospf message-digest-key

Use this command to configure the MD5 authentication key in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf message-digest-key *key-id* **md5** [**0** | **7**] *key*

no ip ospf message-digest-key *key-id*

Parameter Description

Parameter	Description
<i>key</i>	Key of up to 16 characters
0	Displays the key in plain text.
7	Displays the key in cipher text.
<i>key-id</i>	Key identifier in the range from 1 to 255

Defaults No MD5 key is configured by default.

Command Interface configuration mode

Mode

Usage Guide The **ip ospf message-digest-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighboring relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key. For neighbors, the same key identifier must correspond to the same key.

To enable OSPF area authentication, execute the **area authentication** command in routing process configuration mode. The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

The RGOS software supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF packets by using different keys, till it confirms that the neighbors have been configured with new keys. When all devices have been configured with new keys, it is possible to delete the old key.

Configuration Examples The following example adds a new OSPF authentication key "hello5" with key ID 5 for fastEthernet 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication message-digest
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 10 md5 hello10
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5md5 hello5
```

When all neighbors are added with new keys, the old keys shall be deleted for all devices.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip ospf message-digest-key 10md5
hello10
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode.
ip ospf authentication	Enables authentication on the interface and defines authentication mode.

Platform N/A

Description

2.36 ip ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database description

packet. Use the **no** form of this command to restore the default setting.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameter Description	Parameter	Description
	N/A	N/A

Defaults MTU check is disabled by default.

Command

Mode Interface configuration mode

Usage Guide After receiving the database description packet, the device will check whether the MTU of the neighbor interface is the same as its own MTU. If the received database description packet indicates an MTU greater than the interface's MTU, the neighboring relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration The following example disables the MTU check function on fastEthernet 0/1.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf mtu-ignore
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.37 ip ospf network

Use this command to configure the OSPF network type in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf network { broadcast | non-broadcast |

point-to-multipoint [non-broadcast] | point-to-point }

no ip ospf network

Parameter Description	Parameter	Description
	broadcast	Sets the OSPF network type as the broadcast type.
	non-broadcast	Sets the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
	point-to-multipoint [non-broadcast]	Sets the OSPF network type as the point-to-multipoint type. The value is the point-to-multipoint broadcast type by default. The

	non-broadcast option means the point-to-multipoint non-broadcast type.
point-to-point	Sets the OSPF network type as the point-to-point type.

Defaults

The default configurations are as follows:

PTP network type: Point-to-Point Protocol(PPP), Serial Line Internet Protocol(SLIP), frame relay point-to-point (PTP) sub-interface, X.25 PTP sub-interface encapsulation

NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface)

Broadcast network type: Ethernet encapsulation

By default, the network type is the point-to-multipoint network type.

Command

Mode Interface configuration mode

Usage Guide

The broadcast type requires that the interface must have the broadcast capability.

The P2P type requires that the interfaces are interconnected in one-to-one manner.

The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other.

The P2MP type does not raise any requirement.

Configuration

The following example configures the frame relay interface network as the P2P type.

Examples

```
Ruijie(config)# interface Serial 1/0
Ruijie(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0
Ruijie(config-Serial 1/0)# encapsulation frame-relay
Ruijie(config-Serial 1/0)# ip ospf network point-to-point
```

The following example configures the frame relay interface network as the NBMA type.

```
Ruijie(config)# interface Serial 1/0
Ruijie(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0
Ruijie(config-Serial 1/0)# encapsulation frame-relay
Ruijie(config-Serial 1/0)# ip ospf network non-broadcast
Ruijie(config-Serial 1/0)# exit
Ruijie(config)# router ospf 20
Ruijie(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
dialer map ip	Defines the mapping between IP address and dialing number.
frame-relay map	Defines the mapping between IP address and frame DLCI.
neighbor(OSPF)	Defines the IP address of neighbor applicable to NBMA network type and point-to-multipoint non-broadcast type only.

X25 map	Defines the mapping between IP address and X.25 network address.
----------------	--

Platform N/A

Description

2.38 ip ospf priority

Use this command to configure the OSPF priority in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf priority *priority*

no ip ospf priority

Parameter Description	Parameter	Description
	<i>priority</i>	Sets the OSPF priority of the interface in the range from 0 to 255.

Defaults The default is 1.

Command

Mode Interface configuration mode

Usage Guide The interface priority is included in the Hello packet. When DR/BDR election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid only for OSPF broadcast and non-broadcast network types.

Configuration The following example configures the priority of fastethernet 0/1 as 0.

Examples

```
Switch(config)#interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ipospfpriority0
```

Related Commands	Command	Description
	ip ospf network	Configures the network type of the interface.

Platform N/A

Description

2.39 ip ospf retransmit-interval

Use this command to define the interval for sending the link state update (LSU) packet on the interface in interface configuration mode. Use the **no** form of this command to restore the default

setting.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter Description	Parameter	Description
	<i>seconds</i>	Interval for sending the LSU packets in seconds. The range is from 1 to 65535. This interval must be greater than the round trip delay of packets between two neighbors.

Defaults The default is 5.

Command

Mode Interface configuration mode

Usage Guide After the device sends an LSU packet, the LSU packet stays in the transmission buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the **ip ospf retransmit-interval** command, the LSU will be sent once again.

In serial lines or virtual links, the retransmission interval shall be slightly larger. The LSU packet retransmission interval of virtual links is defined with the area virtual-link command followed with the keyword retransmit-interval.

Configuration Examples The following example configures the LSU packet retransmission interval on fastEthernet 0/1 as 10 seconds.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10
```

Related Commands	Command	Description
	area virtual-link	Defines an OSPF virtual link.

Platform N/A

Description

2.40 ip ospf source-check-ignore

Use this command to disable the source address check in the point-to-point link. Use the **no** form of this command to restore the default setting

ip ospf source-check-ignore

no ip ospf source-check-ignore

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command

Mode Interface configuration mode

Usage Guide For OSPF, the source address of the received packet is required to be in the same network segment with the receiving interface. However, in a point-to-point link, the addresses of two ends of the link are individually set, and they are not required to be in the same network segment. The peer address is informed during the process of point-to-point link negotiation; therefore, OSPF will check whether the source address of the packet is the informed one. If no, the OSPF regards this packet as illegal and drops it. In some applications, the addresses informed during the negotiation are shielded. You need to disable the source address check to ensure the normal establishment of OSPF neighbors. The source address check shall be never enabled, especially for the unnumbered interfaces.

Configuration The following example disables the source address check function in the point-to-point link.

Examples

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# ip ospf source-check-ignore
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

2.41 ip ospf subvlan

Use this command to enable OSPF on super VLANs. Use the **no** form of this command to restore the default setting.

ip ospf subvlan [all | vid]

no ip ospf subvlan

**Parameter
Description**

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults The default setting takes effect only on super VLANs with OSPFv3 disabled.

Command

Mode Interface configuration mode

Usage Guide In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are

also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the OSPF function does not need to be enabled on a super VLAN. Therefore, the OSPF function is disabled by default. However, in some scenarios, the OSPF function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration The following example sends OSPF multicast packets to sub VLAN 1024 of super VLAN 300.

Examples

```
Ruijie(config)# interface vlan 300
Ruijie(config-if-VLAN 300)# ip ospf subvlan 1024
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

2.42 ip ospf transmit-delay

Use this command to define the LSU packet transmission delay in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter Description

Parameter	Description
<i>seconds</i>	LSU packet transmission delay in seconds in the range from 1 to 65535.

Defaults

The default is 1.

Command Mode

Interface configuration mode

Usage Guide

Before the LSU packet is transmitted, the Age field in all the LSAs of the packet will be increased by the value defined with the **ip ospf transmit-delay** command in interface configuration mode. The configuration of this parameter shall consider the transmission and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU

packet transmission delay of the virtual link is defined with the **area virtual-link** command followed with the keyword `retransmit-interval`.

The RGOS software will resend or request resending the LSA with Age up to 3600. If no update is obtained in time, the aged LSA will be cleared from the link state database.

Configuration The following example configures the transmission delay of fastEthernet 0/1 as 10.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10
```

**Related
Commands**

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform N/A

Description

2.43 ispf enable

Use this command to enable the ISPF function. Use the **no** form of this command to disable the ISPF function.

ispf enable

no ispf enable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults ISPF is disabled by default.

Command

Mode Routing process configuration mode

Usage Guide

OSPF adopts the SPF algorithm to calculate the network topology within an area. SPF algorithm is run for each area independently,

Incremental SPF algorithm (ISPF) is an area-based algorithm, If the topology changes, the ISPF algorithm will calculate only the affected notes of the topology rather than calculating the entire tree, which speeds up the OSPF route convergence and saves CPU resources.

Because the ISPF algorithm is not shared among routers, each router within the same network can have a unique ISPF algorithm. To ensure a faster OSPF convergence, the ISPF function should be enabled on every router within the network.

Enabling ISPF function only affects the choice of topology calculating algorithm for OSPF. So you can configure the delay time for the ISPF with the **timers spf** command and the **timers throttle spf** command as well.

Configuration The following example enables the ISPF function.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# ispf enable
```

The following example enables the ISPF function on the specified VRF.

```
Ruijie(config)# router ospf 1 vrf vpn1
Ruijie(config-router)# ispf enable
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

2.44 log-adj-changes

Use this command to enable the logging of the neighbor state changes. Use the **no** form of the command to disable this function.

log-adj-changes [detail]

no log-adj-changes [detail]

**Parameter
Description**

Parameter	Description
detail	Records the detail of changes.

Defaults

This function is enabled by default. Without the detail parameter, the system records the logs that the neighbor enters or exits the full state.

Command

Mode Routing process configuration mode

Usage Guide N/A

Configuration The following example logs the neighbor state changes.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# log-adj-changes detail
```

**Related
Commands**

Command	Description
show ip ospf	Displays the OSPF global configuration information.

Platform N/A

Description

2.45 max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description	Parameter	Description
	<i>number</i>	Maximum number of DD packets in the range from 1 to 65535

Defaults The default is 5.

Command

Mode Routing process configuration mode

Usage Guide When a router is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have at the same time.

Configuration The following example sets the maximum number of DD packets to 4.

Examples After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
Ruijie(config)# routerospf10
Ruijie(config-router)# max-concurrent-dd4
```

Related Commands	Command	Description
	router ospf max-concurrent-dd	Sets the maximum number of neighbors allowed in concurrent interaction for all OSPF routing processes.

Platform N/A

Description

2.46 max-metric

Use this command to set the maximum metric of the router-lsa, so that this routing device will not firstly be used as the transmission node by other devices in SPF computing. Use the **no** form of this command to restore the default setting.

max-metric router-lsa [**external-lsa** [*max-metric-value*]][**include-stub**][**on-startup** [*seconds*]][**summary-lsa** [*max-metric-value*]]

no max-metric router-lsa [**external-lsa** [*max-metric-value*]][**include-stub**][**on-startup**

[*seconds*]][**summary-lsa** [*max-metric-value*]]

Parameter Description	Parameter	Description
	router-lsa	Configures the maximum metric (0XFFFF) of non-stub links in the Router LSA.
	external-lsa	Uses the maximum metric instead of the external-lsa metric (including the Type-5 and Type-7).
	<i>max-metric-value</i>	Maximum metric of the LAS. The range is 1 to 16777215. The default value is 16711680,
	include-stub	Configures the maximum metric of the stub links in the Router LSA.
	on-startup	Advertises the maximum metric when the routing device starts up.
	<i>seconds</i>	Interval of advertising the maximum metric. The range is 5 to 86400. The default value is 600 seconds.
	summary-lsa	Uses the maximum metric to replace the summary LSA metric. (including Type-3 and Type-4)

Defaults The normal metric LSAs are used by default.

Command

Mode Routing process configuration mode

Usage Guide With the **max-metric router-lsa** command enabled, the maximum metric of non-stub links in the Router LSA generated by the routing device is set. The link's normal metric is restored after canceling this configuration or reaching the timer.

By default, with this command enabled, the normal metric of the stub links is still advertised, which is the output interface cost. If the **include-stub** parameter is configured, the maximum metric of the stub links will be advertised.

When the device acts as an ABR, if no interval flow transmission is expected, use the **summary-lsa** parameter to set the summary LSA as the maximum metric.

When the device acts as an ASBR device, if no external flow transmission is expected, use the **external lsa** parameter to set the external LSA as the maximum metric.

The **max-metric router-lsa** command is usually used in the following scenes:

The device is restarted, which generally makes the IGP protocol converge faster, so that other devices attempt forwarding the dataflow through the new started-up device. If the current device remains establishing a BGP routing table, the packets sent to these networks will be discarded due to some BGP routings have not been learned. In this case, use the **on-startup** parameter to set certain delay, so that this device can serve as a transmission node after restarting.

The device is added into the network without being used for dataflow transmission. If the backup path exists, the current device is not used for the dataflow transmission. Otherwise, this device is still used to transmit the dataflow.

Remove the device from the network gracefully. With this command enabled, the current device advertises the maximum metric to all devices, as that the other devices in this network can choose the backup path to for the dataflow transmission before the current device is removed.

- i** For the OSPF implementation in the earlier versions (RFC 1247 or earlier versions), the links with the maximum metric (0xFFFF) in the LSA will not participate in the SPF calculation, that is, no dataflow will be sent to the router that have generated these LSAs.

Configuration The following example configures the LSA maximum metric as 100 seconds after starting the device.

Examples

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# max-metric router-lsa on-startup 100
```

**Related
Commands**

Command	Description
show ip ospf	Displays the OSPF related configurations.

Platform N/A
Description

2.47 neighbor

Use this command to define the OSPF neighbor in routing process configuration mode. Use the **no** form of this command to restore the default setting.

Neighbor *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost*]
no neighbor *ip-address* [[**poll-interval**] [**priority**] [*cost*]]

**Parameter
Description**

Parameter	Description
<i>ip address</i>	IP address of the neighbor
poll-interval <i>seconds</i>	(Optional) Specifies the interval of polling neighbors in seconds. The range is from 0 to 2147483647. Only the non-broadcast (NBMA) network type supports this option.
priority <i>priority</i>	(Optional) Configures the priority of non-broadcast network neighbors. The range is from 0 to 255. Only the non-broadcast (NBMA) network type supports this option.
cost <i>cost</i>	(Optional) Configures the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. The range is from 0 to 65535. Only the point-to-multipoint [non-broadcast] network type supports this option.

Defaults No neighbor is defined by default.
The default neighbor polling interval is 120 seconds.
The default NBMA neighbor priority is 0.

Command

Mode Routing process configuration mode

Usage Guide The RGOS software must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface.

In the NBMA network, if the neighbor device becomes inactive, in other words, if the Hello packet is not received within the device dead-interval, the OSPF will send more Hello packets to the neighbor. The interval at which the Hello packets are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello packets only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello packets to all neighbors to establish the neighbor relationship.

Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the cost option for the point-to-multipoint network type.

Configuration Examples The following example declares an OSPF non-broadcast network neighbor, with the IP address 172.16.24.2, priority 1 and polling interval 150 seconds.

```
Ruijie(config)# routerospf 20
Ruijie(config-router)# network 172.16.24.0 0.0.0.255 area 0
Ruijie(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
ip ospf priority	Sets the interface priority.
ip ospf network	Sets the network type

Platform N/A

Description

2.48 network area

Use this command to define which interfaces run OSPF and the OSPF areas they belong to in routing process configuration mode. Use the **no** form of this command to restore the default setting.

network *ip-address wildcard area area-id*

no network *ip-address wildcard area area-id*

Parameter Description

Parameter	Description
<i>ip-address</i>	IP address of the interface
<i>wildcard</i>	Defines the comparison bits in the IP address, with 0 for exact match and 1 for no comparison
<i>area-id</i>	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as

	the OSPF area identifier.
--	---------------------------

Defaults No OSPF area is configured by default.

Command

Mode Routing process configuration mode

Usage Guide The ip-address and wildcard parameters allow associating multiple interfaces with one OSPF area. To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by the network area command. If only the secondary IP address is included, OSPF cannot be enabled on the interface. You can determine the OSPF process that the interface takes part in by the means of the best match if the IP address of the interface matches the IP address ranges defined by the network command in multiple OSPF processes.

Configuration The following example defines:

Examples Three areas: 0, 1 and 172.16.16.0

The interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1

The interfaces whose IP addresses fall into the 172.16.16.0/20 range to area 2

The remaining interface being assigned to area 0.

```
Ruijie(config)# routerospf 20
Ruijie(config-router)# network172.16.16.0
0.0.15.255 area172.16.16.0
Ruijie(config-router)# network192.168.12.0
0.0.0.255 area 1
Ruijie(config-router)# network0.0.0.0 255.255.255.255 area0
```

**Related
Commands**

Command	Description
router ospf	Creates the OSPF routing process.

Platform N/A

Description

2.49 overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance. Use the **no** form of this command to restore the default setting.

overflow database *number* [**hard** | **soft**]

no overflow database

**Parameter
Description**

Parameter	Description
<i>number</i>	Maximum number of LSAs. The range is from 1 to 4294967294.

hard soft	hard: shuts down the OSPF instance when the number of LSAs exceeds that number. soft: issues an alarm when the number of LSAs exceeds that number.
--------------------	---

Defaults The maximum number of LSAs supported by the current OSPF instance is not restricted by default.

Command

Mode Routing process configuration mode

Usage Guide To shut down the OSPF instance when the number of LSAs exceeds that number, use the hard parameter; otherwise, use the soft parameter.

Configuration Examples The following example configures that OSPF instance 10 will be shut down when there are more than 10 LSAs.

```
Ruijie(config)# router ospf 10
Ruijie(config-router)# overflow database 10 hard
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.50 overflow database external

Use this command to configure the maximum number of external LSAs and the waiting time from the overflow state to the normal state. Use the **no** form of this command to restore the default setting.

overflow database external *max-dbsize* *wait-time*

no overflow database external

Parameter Description


Parameter	Description
<i>max-dbsize</i>	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS). The range is from 0 to 2147483647.
<i>wait-time</i>	Waiting time of the routing device from the overflow status to normal status. The range is from 0 to 2147483647.

Defaults The maximum number of external-LSAs is not restricted by default.
If the maximum number of external-LSAs is restricted, the normal status cannot be restored when the maximum number is exceeded.


Command Routing process configuration mode


Mode

Usage Guide When the number of external-LSAs exceeds the value of max-db size, the device enters the overflow state. Then no more external-LSA will be loaded and the external-LSAs generated locally will be cleared. After wait-time expires, the device restores to the normal state and external-LSAs are reloaded.

 When using this function, ensure that all routers of the OSPF backbone area and common areas use the same max-db size value. Otherwise, the following situations occur:

 The link status is inconsistent on the entire network and neighbors fail to achieve the Full state.

 Incorrect routes occur, including loops.

 AS-External-LSAs may be frequently retransmitted.

Configuration Examples The following example configures that the maximum number of external LSAs is 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow state to the normal state is 3 seconds.

```
Ruijie(config)# routerospf10
Ruijie(config-router)# overflow database external10 3
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

2.51 overflow memory-lack

Use this command to allow OSPF to enter the OVERFLOW state when the memory lacks. Use the **no** form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default

Command

Mode Routing process configuration mode

Usage Guide The action of OSPF entering the OVERFLOW state is to discard the newly-learned external route and

effectively prevent the memory from increasing.

It is possible that enabling this function causes the route loop in the whole network. To reduce that possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state.

Use the **clear ip ospf process** command to reset the OSPF and remove the OSPF OVERFLOW state.

Use the no form of this command to prevent the OSPF to enter the OVERFLOW state when the memory is insufficient, which may result in the constantly consumption of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.

Configuration The following example prevents the OSPF from entering the OVERFLOW state when the memory is insufficient.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no overflow memory-lack
```

**Related
Commands**

Command	Description
clear ip ospf process	Resets the OSPF instances.
show ip protocols ospf	Displays the OSPF information.

Platform N/A

Description

2.52 passive-interface

Use this command to configure the specified network interface or all interface as the passive interfaces. Use the **no** form of this command to restore the default setting.

passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ip-address* }

no passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ip-address* }

**Parameter
Description**

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Interface to be set as a passive interface
default	Sets all the interfaces as passive interfaces
<i>interface-type</i> <i>interface-number</i> <i>ip-address</i>	Sets the address of the specified interface as a passive address.

Defaults No interface is configured as a passive interface by default. All interfaces are allowed to receive or send OSPF packets.

Command**Mode** Routing process configuration mode**Usage Guide** To prevent other devices in the network from dynamically learning the routing information of the device, set the specified network interface of this device as a passive interface or the IP address of the specified network interface as a passive address**Configuration Examples** The following example configures fastEthernet 0/1 as a passive interface and the IP address of the interface 1.1.1.1 as the passive address.

```
Ruijie(config)# routerospf 30
Ruijie(config-router)# passive-interface fastEthernet 0/1
Ruijie(config-router)# passive-interface fastEthernet 0/1 1.1.1.1
```

Related Commands

Command	Description
show ip ospf interface	Displays the configuration information of the interface.

Platform N/A**Description**

2.53 redistribute

Use this command to redistribute the external routing information. Use the **no** form of this command to restore the default setting.

```
redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | rip | static } [ { level-1 | level-1-2 | level-2 } ] [ match { internal | external [ 1|2 ] | nssa-external [ 1|2 ] } ] [ metric metric-value ] [ metric-type { 1|2 } ] [ route-map route-map-name ] [ subnets ] [ tag tag-value ]
no redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | rip | static } [ { level-1 | level-1-2 | level-2 } ] [ match { internal | external [ 1|2 ] | nssa-external [ 1|2 ] } ] [ metric metric-value ] [ metric-type { 1|2 } ] [ route-map route-map-name ] [ subnets ] [ tag tag-value ]
```

Parameter Description

Parameter	Description
bgp	Redistribution from bgp
connected	Redistribution from direct routes
isis [<i>area-tag</i>]	Redistribution from an IS-IS instance specified in area-tag
ospf <i>process-id</i>	Redistribution from an ospf instance specified in process-id in the range from 1 to 65,535
rip	Redistribution from rip
static	Redistribution from static routes
level-1 level-1-2 level-2	Configures IS-IS route redistribution. The parameter specifies a level,

	and routes of this level will be redistributed. Only level-2 IS-IS routes can be redistributed by default.
match	Filters specified routes for configuring OSPF route redistribution. By default, all the OSPF routes are redistributed.
metric <i>metric-value</i>	Specifies the metric of an OSPF external LSA in the range from 0 to 16777214.
metric-type {1 2}	Sets the external routing type as E-1 or E-2.
route-map <i>route-map-name</i>	Redistribution filter rule
subnets	Redistributes the routes of non standard networks.
tag <i>tag-value</i>	Sets the tag value of the routes redistributed to the OSPF in the range from 0 to 4294967295.

Defaults

Redistribution configuration is not supported by default.

If you configure OSPF redistribution, all subtype routes of the instance are redistributed.

If you configure ISIS redistribution, all level-2 subtype routes of the instance are redistributed.

In other cases, all routings of this type are redistributed.

The default metric of the redistribution BGP route is 1. The default metric of LSAs generated by routes of other types is 20.

The default value of metric-type is E-2.

No route-map is associated by default.

Command**Mode**


Route configuration mode


Usage Guide

After the command is configured, the router will become an ASBR, and the related routing information is imported into the OSPF domain and broadcasted to other OSPF routers through type-5 LSAs.

When you configure is route redistribution without the level parameter, level-2 routes can be redistributed by default. In initial redistribution configuration that carries the level parameter, routes of the specified level can be redistributed. When you save the configuration containing both level 1 and level 2, they are merged into level-1-2 for convenience. For details, see the configuration examples. When you configure OSPF router distribution without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. Use the no form of this command to restore the default configuration.

When you filter routes for redistribution by following the route-map rule, the match rule of the route-map rule is specific for the original redistribution parameters. The route-map rule works only when the redistributed OSPF routes follow the match rule.

 The range of set metric is from 0 to 16777214 for the associated route-map. If the value exceeds the range, introducing a route fails.

 The following are the rules for configuring the no form of the redistribute command:1. If the **no** form specifies some parameters, restore their default values.2. If the **no** form contains no parameter, delete the whole command. If the following configuration exists: redistribute isis 112 level-2 You can use the no redistribute isis 112 level-2command to modify the configuration.

According to preceding rules, this command restores the level-2 parameter to the default value, namely level-2. Therefore, the configuration remains the same after the no form of the preceding command is executed. redistribute isis 112 level-2 To delete the whole command, use the following command: no redistribute isis 112

Configuration Examples The following example redistributes routes of **ospf2** and **isis** isis-001 to the OSPF area.

Examples

```
Ruijie(config)# router ospf1
Ruijie(config-router)# redistribute ospf 2 subnets
Ruijie(config-router)# redistribute ospf2match
external 1 internal
Ruijie(config-router)# redistribute isisis-001
Ruijie(config-router)# redistribute isisis-001 level-1
```

The following example displays the output of the **show run** command.

```
router ospf 1
redistribute ospf 2 match external 1 internal subnets
redistribute isis isis-001 level-1-2
```

Related Commands

Command	Description
summary-address	Configures the aggregate route for the external route of the OSPF route area.
default-metric	Sets the default metric of the OSPF redistribution route.

Platform N/A

Description

2.54 router ospf

Use this command to create the OSPF routing process in global configuration mode. Use the **no** form of this command to restore the default setting.

router ospf

router ospf *process-id* [**vrf** *vrf-name*]

no router ospf *process-id*

Parameter Description

Parameter	Description
<i>process-id</i>	ID of an OSPF process. If the process ID is not configured, process 1 is configured.
<i>vrf-name</i>	VRF of the configured OSPF process for products that support the VRF.

Defaults No OSPF routing process exists by default.

Command**Mode** Global configuration mode**Usage Guide** Based on the original implementation, the RGOS10.1 adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.**Configuration** The following example creates the OSPF routing process 10 within the specified vrf: vpn_1.**Examples**

```
Ruijie(config)# router ospf10 vrf: vpn_1
```

**Related
Commands**

Command	Description
show ip protocols	Displays the routing protocol information.
show ip ospf	Displays the OSPF information.

Platform N/A**Description**

2.55 router ospf max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

router ospf max-concurrent-dd *number***no router ospf max-concurrent-dd****Parameter
Description**

Parameter	Description
<i>number</i>	Maximum number of DD packets in the range from 1 to 65535.

Defaults The default is 10.**Command****Mode** Global configuration mode**Usage Guide** When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have (initiated or accepted) at the same time.**Configuration** The following example sets the maximum number of DD packets to 4.**Examples** After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
Ruijie# configure terminal
Ruijie(config)# router ospfmax-concurrent-dd4
```


Related Commands	Command	Description
		max-concurrent-dd

Platform N/A
Description

2.56 router-id

Use this command to set the router ID. Use the **no** form of this command to restore the default setting.

router-id *router-id*
no router-id

Parameter Description	Parameter	Description
		<i>router-id</i>

Defaults The OSPF routing process will select the maximal interface IP address as the router ID by default. If the loopback interface of an IP address is not configured, the OSPF routing process will select the maximum IP address among all its physical interfaces as the router ID.

Command

Mode Routing process configuration mode

Usage Guide You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a lot of processing. Therefore, it is not recommended to change the router ID. The device can be changed only when no LSA is generated.

Configuration The following example modifies the router ID to 0.0.0.36.

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# router-id 0.0.0.36
```

Related Commands	Command	Description
		show ip protocols

Platform N/A
Description

2.57 show ip ospf

Use this command to display the OSPF information.

show ip ospf [*process-id*]

Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command displays the information of the OSPF routing process.

Configuration The following example displays the output of the **show ip ospf** command.

Examples

```
Ruijie# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Domain ID type 0x0105, value 0x010101010101
Process uptime is 4 minutes
Process bound to VRF default
Memory Overflow is enabled.
Router is not in overflow state now.
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Enable two-way-maintain
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Originating router-LSAs with maximum metric
Condition:on startup for 100 seconds, State:inactive
Advertise stub links with maximum metric in router-LSAs
Advertise summary-LSAs with metric 16711680
Advertise external-LSAs with metric 16711680
Unset reason:timer expired, Originated for 100 seconds
Unset time:00:02:02.080, Time elapsed: 00:23:54.656
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Initial LSA throttle delay 0 msec
Minimum hold time for LSA throttle 5000 msec
Maximum wait time for LSA throttle 5000 msec
Lsa Transmit Pacing timer 40 msec, 10 LS-Upd
Minimum LSA arrival 1000 msec
Pacing lsa-group:240 secs
```

```

Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjacency Changes :Enabled
Graceful-restart disabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
BFD enabled
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
Number of LSA 3. Checksum 0x0204bf
Area 1 (NSSA)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
Area has no authentication
SPF algorithm last executed 02:09:23.040 ago
SPF algorithm executed 4 times
Number of LSA 6. Checksum 0x028638
NSSA Translator State is disabled, Stability Interval expired in 00:00:03

```

Field	Description
Router ID	ID of a router.
Process uptime	Effective time of the current OSPF process (the process does not take effect when device-id is 0.0.0.0)
Bou to VRF	VRF of the current OSPF
Conforms to RFC2328	Same as the RFC2328
RFC1583Compatibilit flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external routes. This policy is used in the selection of best ASBR and in the route comparison.

Support Tos	Supports Only TOS0.
Supports opaque LSA	Supports opaque-LSA.
Graceful-restart	GR Restart capability described in the RFC3623 Graceful Restart
Graceful-restart helper	GR Help capability described in the RFC3623 Graceful Restart
Router Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	Parameter used for LSA pacing, checksum calculation, and aging interval
Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.
Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled

Number of areas attached to this router	Total number of areas on the devices
Area type	Area type, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSATranslatorState	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA.
BFD enabled	Enables BFD for OSPF.

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

2.58 show ip ospf border-routers

Use this command to display the OSPF internal routing table on the ABR/ASBR.

show ip ospf [*process-id*] border-routers

**Parameter
Description**

Parameter	Description
<i>process-id</i>	OSPF process ID

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command displays the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the `show ip route` command. The OSPF internal routing table has the destination address of the router ID instead of the destination network.

Configuration The following example displays the output of the **show ip ospf border-mrouters** command.

Examples

```
Ruijie# show ip ospf border-routers
OSPF internal Routing Table
Codes:i - Intra-area route, I - Inter-area route
i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select
The following table describes fields in the output.
```

Field	Description
Codes	Route type code, where "i" means intra-area routes, while "I" means inter-area routes.
I	Intra-area routes
1.1.1.1	Displays the OSPF ID of the border device.
[2]	Displays the cost to the border device.
via 10.0.0.1	Displays the next-hop gateway to the border device.
FastEthernet 0/1	Displays the interface to the border device.
ABR, ASBR	Displays the type of the border device, including ABR, ASBR, or both.
Area 0.0.0.1	Displays the area that learns the route.
select	Indicates the currently selected optimal path when there are multiple paths to the ASBR.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.59 show ip ospf database

Use this command to display the OSPF link state database information. Use the **no** form of this command to restore the default setting. Different formats of the command will display different LSA information.

```
show ip ospf [ process-id [ area-id | ip-address ] ] database [ { asbr-summary | external | network |
nssa-external | opaque-area | opaque-as | opaque-link | router | summary } ] [ { adv-router
ip-address | self-originate } | link-state-id | brief ] [ database-summary | max-age | detail ]
```

Parameter Description	Parameter	Description
	<i>area-id</i>	(Optional) Displays the area ID.
	adv-device	(Optional) Displays the LSA information generated by the specified advertising device.
	<i>link-state-id</i>	(Optional) Displays the LSA information of the specified OSPF link state identifier.
	self-originate	(Optional) Displays the LSA information generated by the device itself.
	Max-age	(Optional) Displays the LSAs aged.
	router	(Optional) Displays the OSPF device LSA information.
	network	(Optional) Displays the OSPF network LSA information.
	summary	(Optional) Displays the OSPF summary LSA information.
	asbr-summary	(Optional) Displays the ASBR summary LSA information.
	external	(Optional) Displays the OSPF external LSA information.
	nssa-external	(Optional) Displays the category 7 OSPF external LSA information.
	opaque-area	(Optional) Displays type 10 LSAs.
	opaque-as	(Optional) Displays type 11 LSAs.
	opaque-link	(Optional) Displays type 9 LSAs.
	database-summary	(Optional) Displays the statistics of LSAs of the link state database.
	detail	Displays detailed information of LSAs of the OSPF.
	brief	Displays the brief information of the LSAs of the specified type.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide When the OSPF link state database is very large, you should display the information on the link state database by item. Proper use of commands may help OSPF troubleshooting.

Configuration The following example displays the output of the **show ip ospf database** command.

Examples

```
Ruijie# show ip ospf database
OSPF Device with ID (1.1.1.1) (Process ID 1)
Device Link States (Area 0.0.0.0)
Link ID      ADV Device    Age  Seq#      CkSum  Link count
1.1.1.1      1.1.1.1       2   0x80000011 0x6f39  2
3.3.3.3      3.3.3.3      120 0x80000002 0x26ac  1
Network Link States (Area 0.0.0.0)
Link ID      ADV Device    Age  Seq#      CkSum
```

```

192.88.88.27  1.1.1.1      120  0x80000001  0x5366
Summary Link States (Area 0.0.0.0)
Link ID      ADV Device    Age  Seq#      CkSum  Route
10.0.0.0    1.1.1.1      2   0x80000003 0x350d 10.0.0.0/24
100.0.0.0   1.1.1.1      2   0x8000000c 0x1ecb 100.0.0.0/16
Device Link States (Area 0.0.0.1 [NSSA])
Link ID      ADV Device    Age  Seq#      CkSum  Link count
1.1.1.1     1.1.1.1      2   0x80000001 0x91a2 1
      Summary Link States (Area 0.0.0.1 [NSSA])
Link ID      ADV Device    Age  Seq#      CkSum  Route
100.0.0.0   1.1.1.1      2   0x80000001 0x52a4 100.0.0.0/16
192.88.88.0 1.1.1.1      2   0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID      ADV Device    Age  Seq#      CkSum  Route      Tag
20.0.0.0    1.1.1.1      1   0x80000001 0x033c  E2 20.0.0.0/24  0
100.0.0.0   1.1.1.1      1   0x80000001 0x9469  E2 100.0.0.0/28 0
AS External Link States
Link ID      ADV Device    Age  Seq#      CkSum  Route      Tag
20.0.0.0    1.1.1.1      380 0x8000000a 0x7627  E2 20.0.0.0/24  0
100.0.0.0   1.1.1.1      620 0x8000000a 0x0854  E2 100.0.0.0/28  0

```

The following table describes the fields in the output of the **show ip ospf database** command.

Field	Description
OSPF Device with ID	Displays the Router ID.
Device Link States	Displays the device LSA information.
Net Link States	Displays the network LSA information.
Summary Net Link States	Displays the summary network LSA information.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
AS External Link States	Displays the type 5 autonomous external LSA information.
Link ID	Displays the Link ID.
ADV Device	Displays the ID of the device that advertises the LSAs.
Age	Displays the keepalive period of the LSA.
Seq#	Displays the sequence number of the LSA, which is used to check aged or duplicate LSAs.
Cksum	Displays the checksum of LSAs.
Link-Count	Displays the number of links in the device LSA information.
Route	Displays the device information included in the LSA.
Tag	Displays the tag of the LSA.

The following example displays the output the **show ip ospf database asbr-summary** command.


```

Ruijie# show ip ospf database asbr-summary
      OSPF Device with ID (1.1.1.35) (Process ID 1)
        ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Device address)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
      TOS: 0 Metric: 1

```

The following table describes the fields in the output of the **show ip ospf database asbr-summary** command.

Field	Description
OSPF Device with ID	Displays the router ID.
AS Summary Link States	Displays the summary LSA information in the AS.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
AdvertisingRouter	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be only 0 now.
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database external** command.

```

Ruijie# show ip ospf database external
      OSPF Device with ID (1.1.1.35) (Process ID 1)
        AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627

```

```

Length: 36
Network Mask: /24
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 0

```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-5 AS External Link States	Displays autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Indicates the external link type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used by other routing processes to redistribute OSPF routes.

The following example displays the output of the **show ip ospf database network** command:

```

Ruijie# show ip ospf database network
OSPF Router with ID (1.1.1.1) (Process ID 1)
Network Link States (Area 0.0.0.0)
LS age: 572
Options:0x2 (*|---|---|E|)
LS Type:network-LSA
Link State ID:192.88.88.27 (address of Designated Router)

```

```

Advertising Router:1.1.1.1
LS Seq Number: 80000001
Checksum:0x5366
Length: 32
Network Mask: /24
Attached Router:1.1.1.1
Attached Router:3.3.3.3

```

The following table describes the fields in the output of the **show ip ospf database network** command.

Field	Description
OSPF Router with ID	Displays the router ID corresponding to the follow-up information and the process ID corresponding to the OSPF.
Network LinStates	Displays the network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Device	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the network corresponding to the LSA.
Attached Router	Displays the device that is connected with the network.

The following example displays the output of the **show ip ospf database device** command:

```

Ruijie# show ip ospf database router
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
LS age: 322
Options:0x2 (*|-|-|-|-|E|-)
Flags:0x3 :ABR ASBR
LS Type:router-LSA
Link State ID:1.1.1.1
Advertising Router:1.1.1.1
LS Seq Number: 80000012
Checksum:0x6d3a
Length: 48
Number of Links: 2
Link connected to:Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0

```

```
TOS 0 Metric: 0
```

The following table describes the fields in the output of the **show ip ospf database device** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Device Link States	Displays the device LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
Flag	Flag
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Number of Links	Displays the number of links associated with the device.
Link connected to	Displays what the link is connected to and the network type.
(Link ID)	Link identifier
(Link Data)	Link data
Number of TOS metrics	TOS value, supporting TOS0 only
TOS 0 Metrics	TOS0 metric

The following example displays the output of the **show ip ospf database summary** command:

```
Ruijie# show ip ospf database summary
      OSPF Device with ID (1.1.1.1) (Process ID 1)
        Summary Link States (Area 0.0.0.0)
LS age: 499
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
Advertising Device: 1.1.1.1
```

```

LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
    TOS: 0 Metric: 11

```

The following table describes the fields in the output of the **show ip ospf database summary** command.

Field	Description
OSPF Router with ID	Displays the router ID.
Summary Net Link States	Displays the summary network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, supporting only 0 now
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database nssa-external** command:

```

Ruijie# show ip ospf database nssa-external
    OSPF Device with ID (1.1.1.1) (Process ID 1)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 1
Options: 0x0 (*|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001

```

```
Checksum: 0x033c
Length: 36
Network Mask: /24
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 20
    NSSA: Forward Address: 100.0.2.1
    External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database nssa-external** command.

Field	Description
OSPF Router with ID	Displays the router ID.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequential number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.

External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.
--------------------	---

The following example displays the output of the **show ip ospf database external** command:

```
Ruijie# show ip ospf database external
      OSPF Device with ID (1.1.1.1) (Process ID 1)
      AS External Link States
LS age: 1290
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 20
      Forward Address: 0.0.0.0
      External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-7 AS External Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.

Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database database-summary** command:

```
Ruijie# show ip ospf database database-summary
OSPF process 1:
Device Link States      : 4
Network Link States    : 2
Summary Link States     : 4
ASBR-Summary Link States : 0
AS External Link States : 4
NSSA-external Link States: 2
```

The following table describes the fields in the output of the command **show ip ospf database database-summary**.

Field	Description
OSPF Process	OSPF process ID
Router Link	Number of device LSAs in the area
Network Link	Number of network LSAs in the area
Summary Link	Number of summary LSAs in the area
ASBR-Summary Link	Number of ASBR summary LSAs in the area
AS External Link	Number of NSSA LSAs in the area

NSSA-external Link	Number of NSSA LSAs in the area
--------------------	---------------------------------

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.60 show ip ospf interface

Use this command to display the OSPF-associated interface information.

show ip ospf [*process-id*] interface [*interface-type interface-number* | **brief]**

Parameter Description	Parameter	Description
	<i>process-id</i>	
<i>interface-type</i>		(Optional) type of the specified interface
<i>interface-number</i>		(Optional) number of the specified interface
brief		Displays the summary of the interface.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command displays the OSPF information on the interface.

Configuration The following example displays the output of the **show ip ospf interface fastEthernet 0/1** command:

Examples

```
Ruijie# show ip ospf interface fastEthernet0/1
FastEthernet 0/1 is up, line protocol is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500
Matching network config: 192.88.88.0/24
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1,BFD enabled
Designated Router (ID) 1.1.1.1, Interface Address 192.88.88.27
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 70784
Hello received 1786 sent 1787, DD received 13 sent 8
```

```
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

The following table describes the fields in the output of the **show ip ospf interface serial 1/0** command.

Field	Description
FastEthernet 0/1 State	State of the network interface; UP means normal working and Down means faults.
Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router ID	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay
State	DR/BDR state ID
Priority	Priority of the interface
Designated Router(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router ID of the BRD of the interface
BDR's Interface address	Address of the BDR of the interface
Time intervals configured	Hello, Dead, Wait, and Retransmit intervals of the interface
Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of Full neighbors
Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received
DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received
Discard	Statistics on the discarded OSPF packets
BFD enabled	Enables BFD for OSPF.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.61 show ip ospf ispf

Use this command to display the ISPF calculation count in the OSPF area.

show ip ospf [*process-id*] ispf

Parameter Description	Parameter	Description
		<i>process-id</i>

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command displays the ISPF calculation count in the OSPF area within the last 30 minutes and total ISPF calculation count by now.

Configuration The following displays the ISPF calculation count in the OSPF area.

Examples Ruijie# show ip ospf 1 ispf

```
OSPF process 1:
Area_id      30min_counts  Total_counts
0             32                1235
1             6                 356
```

Field Description:

Field	Description
Area_id	OSPF area ID.
30min_counts	ISPF calculation count in the OSPF area within the last 30 minutes.
Total_counts	Total count of ISPF calculation.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.62 show ip ospf neighbor

Use this command to display the OSPF neighbor list.

```
show ip ospf [ process-id ] neighbor [ statistics | { [ interface-type interface-number ] | [ neighbor-id ]
| [ detail ] }
```

Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID
	detail	(Optional) Displays the neighbor details.
	<i>interface-type</i> <i>interface-number</i>	(Optional) Displays the neighbor information of the specified interface
	<i>neighbor-id</i>	(Optional) Displays the information of the specified neighbor
	statistics	(Optional) Displays the neighbor statistics.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command displays neighbor information usually used to check whether the OSPF is running normally.

Configuration The following example displays the output of the **show ip ospf neighbor** command.

Examples

```
Ruijie# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID  Pri  State  BFD State  Dead Time  Address  Interface
3.3.3.3      1   Full/BDR  Up          00:00:32  192.88.88.72
FastEthernet 0/1

Ruijie# show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 192.88.88.72
In the area 0.0.0.0 via interface FastEthernet 0/1
Neighbor priority is 1, State is Full, 11 state changes
DR is 192.88.88.27, BDR is 192.88.88.72
Options is 0x52 (*|O|-|EA|-|-|E|-)
Dead timer due in 00:00:32
Neighbor is up for 05:11:27
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Crypt Sequence Number is 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
```

```

Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timer on
Graceful-restart helper disabled
BFD session state up

```

The following table describes the fields in the output of the **show ip ospf neighbor** command.

Field	Description
Neighbor ID	Neighbor ID
Pri	Neighbor priority (for selection of DR)
State	Neighbor status
Dead Time	Remaining time for the neighbor to enter the Dead status
Address	Interface address of the neighbor
Interface	Interface of the neighbor
interface address	Interface address of the neighbor device
In the area	Displays the area that learns the neighbor.
via interface	Displays the interface that learns the neighbor
Neighbor priority	Priority of the neighbor OSPF
State	OSPF neighbor connection state. FULL means the stable state; DR indicates that the neighbor is the designated device; BDR indicates that the neighbor is the backup designated device; DROTHER indicates that the neighbor is not a DR/BDR. Point-to-point network type has no DR or DBR.
State changes times	Times of state changes
Dead Time	Dead time of the neighbor
DR	Interface address of the DR elected by the neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected by the neighbor device (that is, the BDR field of the Hello packet)
Options	Hello packet E-bit option, where 0 indicates that the area is a STUB area; 2 indicates that the area is not a STUB area.
Dead timer due in	Dead time of the neighbor device
Neighbor up time	Period from when the device is discovered till now
Database Summary List	Statistics on the neighbor DD packets
LinkState Request List	Statistics on the neighbor LS request packets
LinkState Retransmission List	Statistics on the neighbor re-transmit packets

Crypt Sequence Number	Area MD5 authentication code
Thread Inactivity Timer	Status of invalid neighbor timer
Thread Database Description Retransmission	Status of DD packet timer of the interface
ThreadLinkState Request Retransmission	Status of LS request packet timer of the interface
ThreadLinkState Update Retransmission	Status of LS update packet timer of the interface
Thread Poll Timer	Poll Timer start status of the static neighbor
Graceful-restart helper	Whether it is able to function as the GR Helper of a specified neighbor

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

2.63 show ip ospf route

Use this command to display the OSPF routes.

show ip ospf [*process-id*] **route** [**count** | *ip-address mask*]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID. All OSPF routes will be displayed without an ID specified.
count	Statistics of various OSPF routes
<i>ip-address mask</i>	Statistics of routes which have a specified prefix and mask.

Defaults N/A

Command

Mode Privileged mode

Usage Guide This command displays the OSPF routing information. The count option displays the OSPF routing

statistics.

Configuration The following example displays the output of the **show ip ospf route** command.

Examples

```
OSPF process 1:
Codes: C - connected, D - Discard , O - OSPF,
IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 0/1
C 192.88.88.0/24 [1] is directly connected, FastEthernet 0/1, Area 0.0.0.1
```

The following table describes the fields in the output of the **show ip ospf route** command.

Field	Description
codes	Route type and corresponding abbreviation and description
100.0.0.0/24	Route prefix
[1]	Route cost
via	Route next hop and interface

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

2.64 show ip ospf spf

Use this command to display the routing count in the OSPF area.

show ip ospf [*process-id*] spf

**Parameter
Description**

Parameter	Description
<i>process-id</i>	OSPF process ID

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command displays the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.

Configuration The following example displays the output of the **show ip ospf [*process-id*] spf** command:

Examples

```
Ruijie# show ip ospf 1 spf
```

```

OSPF process 1:
Area_id      30min_counts  Total_counts
0             32             1235
1             6             356

```

The following table describes the fields in the output of the **show ip ospf [process-id] spf** command.

Field	Description
Area_id	OSPF area ID
30min_counts	OSPF routing counts within the latest 30 minutes
Total_counts	Total counts of the OSPF routing till now

Related Commands

Command	Description
show ip ospf	Displays the OSPF summary.

Platform N/A
Description

2.65 show ip ospf summary-address

Use this command to display the converged route of all redistributed routes.

show ip ospf [process-id] summary-address

Parameter Description

Parameter	Description
<i>process-id</i>	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command is valid only on the NSSA ABR, and displays only the routes with local aggregation operations.

Configuration The following example displays the output of the **show ip ospf summary-address** command:

Examples

```

Ruijie# show ip ospf summary-address
OSPF Process 1, Summary-address:
172.16.0.0/16, Metric 20, Type 2, Tag 0, Match count 3, advertise

```

Field	Description
Summary Address	IP address to be aggregated

Summary Mask	Mask to be aggregated
Advertise	Whether to advertise the aggregated route
Status	Whether the aggregation range takes effect
Aggregated subnets	Number of external routes included in the aggregation range

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

2.66 show ip ospf topology

Use this command to display topology information for OSPF SPF calculation.

show ip ospf [*process-id* [*area-id*]] **topology** [**adv-router** *adv-router-id* [*router-id*] | **self-originate** [*router-id*]]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID.
<i>area-id</i>	Displayed area ID
topology	Displays a specified OSPF process and topology information summary of an area.
adv-router	Displays topology information of a specified device. This specified device must be a directly connected neighbor of the current device.
self-originate	Displays topology information of the current device.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command helps users to understand OSPF SPF calculation topology information and troubleshoot faults caused by topology planning. If the user enables fast reroute calculation, this command displays information related to fast reroute calculation.

Configuration The following example displays the result of the **show ip ospf topology** command:

Examples

```
Ruijie# show ip ospf topology
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Topology States (Area 0.0.0.0)
+1.1.1.1
+2.2.2.2
```

```

+4.4.4.4
+3.3.3.3
+4.4.4.4

+2.2.2.2
+1.1.1.1
+3.3.3.3
+4.4.4.4
+3.3.3.3

+3.3.3.3
+1.1.1.1
+2.2.2.2
+4.4.4.4
+2.2.2.2

```

The following example displays the result of the **show ip ospf topology self-originate** command:

```

Ruijie# show ip ospf topology self-originate
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Topology States (Area 0.0.0.0)
1.1.1.1
  Self to Destination Metric: 0
Parent Node: -
Child Node:2.2.2.2
  Primary next-hop: -
  Backup next-hop: -
  Backup Neighbor: -

2.2.2.2
  Self to Destination Metric: 1
Parent Node: 1.1.1.1
Child Node:-
  Primary next-hop: FastEthernet 0/1 via 10.0.0.1
  Backup next-hop: FastEthernet 0/2 via 10.0.1.1
  Backup Neighbor: 2.2.2.2
Neighbor to Destination Metric: 0
Neighbor to Self Metric: 10
Neighbor to Primary Neighbor: 0
Self to Neighbor Metric: 1

```

The description of every field displayed by **show ip ospf topology self-originate** is as follows:

Field	Description
Self to Destination Metric	Metric from the root node to the current destination node
Parent Node	Parent node of the current destination node
Child Node	Child node of the current destination node

Primary next-hop	Primary next hop for reaching the current the destination node
Backup next-hop	Backup next hop for reaching the current the destination node
Backup Neighbor	Backup neighbor for reaching the current the destination node
Neighbor to Destination Metric	Metric from the backup neighbor to the current destination node
Neighbor to Self Metric	Metric from the backup neighbor to the root node
Neighbor to Primary Neighbor	Metric from the backup neighbor to the primary neighbor
Self to Neighbor Metric	Metric from the root node to the backup neighbor

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

2.67 show ip ospf virtual-link

Use this command to display the OSPF virtual link information.

show ip ospf [*process-id*] **virtual-link** [*ip-address*]

Parameter Description

Parameter	Description
<i>process-id</i>	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.
<i>ip-address</i>	Associated ID of a virtual link neighbor

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide If no virtual link is configured, the command displays the neighbor status and other related information. The show ip ospf neighbor command does not display the neighbor of the virtual link.

Configuration The following is the output of the **show ip ospf virtual-links** command:

Examples

```
Ruijie# show ip ospf virtual-links
Virtual Link VLINK0 to device 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 0/1
Local address 10.0.0.37/32
Remote address 10.0.0.27/32
```

```
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Adjacency state Full
```

The following table describes the fields in the output.

Field	Description
Virtual Link VLINK0 to router	Displays the virtual link neighbors and their status.
Virtual Link State	Displays the virtual link state.
Transit area	Displays the transit area of the virtual link.
via interface	Displays the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Displays the transmit delay of the virtual link.
State	Interface state
Time intervals configured	Hello, Dead, Wait, and Retransmit interval of the interface
Adjacency State	Neighbor state, where FULL means the stable state

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.68 summary-address

Use this command to configure the aggregate route out of the OSPF routing domain. Use the **no** form of this command to remove the aggregate route.

summary-address *ip-address net-mask* [**not-advertise** | **tag value** | **cost cost**]

no summary-address *ip-address net-mask* [**not-advertise** | **tag** | **cost**]

Parameter Description

Parameter	Description
<i>ip address</i>	IP address of the aggregate route
<i>net-mask</i>	Network mask of the aggregate route
not-advertise	Does not advertise the aggregate route. If the parameter is not configured, the aggregate route is advertised.
tag value	Sets the tag value of an aggregate route. The range is from 0 to 4,294,967,295.

cost <i>cost</i>	Cost value of the aggregate route. The range is from 0 to 16,777,214.
-------------------------	---

Defaults No aggregate route is configured by default.

Command

Mode Routing process configuration mode

Usage Guide When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in external LSAs. If the incoming routes are continuous addresses, the autonomous border device can advertise only one aggregate route, reducing the scale of routing table greatly.

Unlike the **area range** command, the **area range** command aggregates inter-OSPF-area routes, while the **summary-address** command aggregates external routes of the OSPF routing domain.

For the NSSA, the **summary-address** command is valid only on the NSSA ABR now, and aggregates only redistributed routes.

Configuration The following example generates an external aggregate route 100.100.0.0/16.

Examples

```
Ruijie(config)# router ospf20
Ruijie(config-router)# summary-address 100.100.0.0 255.255.0.0
Ruijie(config-router)# redistribute static subnets
Ruijie(config-router)# network 200.2.2.0 0.0.0.255 area 1
Ruijie(config-router)# network 172.16.24.0 0.0.0.255 area 0
Ruijie(config-router)# area nssa
```

Related Commands

Command	Description
area-range	Configures route convergence on the OSPF area border device.
redistribute	Redistributes routes of other routing processes.

Platform N/A

Description

2.69 timers lsa arrival

Use this command to configure the time delay for the same LSA received. Use the **no** form of this command to restore the default setting.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

Parameter	Description
<i>arrival-time</i>	Configures the time delay when receiving the same LSA. The range is from 0 to 600000 in the unit of milliseconds.

Defaults The default is 1000.

Command

Mode Routing process configuration mode

Usage Guide No action is done when the same LSA is received within the specified time.

Configuration The following example configures the time delay for the same LSA as 2seconds.

Examples

```
Ruijie(config)# routerospf1
Ruijie(config-router)# timers arrival-time 2000
```

**Related
Commands**

Command	Description
show ip ospf	Displays the OSPF information.

Platform N/A

Description

2.70 timers pacing lsa-group

Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for the aged link state. Use the **no** form of this command to restore the default setting.

timers pacing lsa-group seconds

no timers pacing lsa-group

**Parameter
Description**

Parameter	Description
seconds	Parameter used for LSA pacing, checksum calculation, and aging interval. The range is from 10 to 1800 in the unit of seconds.

Defaults The default is 30.

Command

Mode Routing process configuration mode

Usage Guide Each LSA has its own update and aging time (LSA age). If you update and age LSAs separately, many CPU resources will be consumed. To effectively use CPU resources, you can update LSAs of a device in batches.

You can use this command to modify the value of seconds, whose default value is 240 seconds. This parameter needs not to be adjusted often. The optimal group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small

database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better.

Configuration The following example configures the pacing time as 120 seconds.

Examples

```
Ruijie(config)# deviceospf 20
Ruijie (config-router)# timers paing lsa-group 120
```

**Related
Commands**

Command	Description
show ip ospf	Displays the OSPF information.

Platform N/A

Description

2.71 timers pacing lsa-transmit

Use this command to transmit the LSA grouping updating. Use the **no** form of this command to restore the default setting.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

**Parameter
Description**

Parameter	Description
<i>transmit-time</i>	Configures the interval of sending the LSA grouping. The range is from 10 to 1000.
<i>transmit-count</i>	Configures the number of LS-UPD packets per group. The range is from 1 to 200.

Defaults The default configurations are as follows:

Transmit-time: 40 milliseconds.

Transmit-count: 1

Command

Mode Routing process configuration mode

Usage Guide If there are a large number of LSAs and the load on the system is heavy, you can properly use the

transmit-time and **transmit-count** to inhibit the flooding LS-UPD packet number in the network.

If the CPU and network bandwidth loads are not too much, reduce **transimi-time** and increase **transimit-count** to quicken the environment convergence.

Configuration Examples The following example sets the interval of sending the LS-UPD packets as 50ms, the packets number as 20.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands	Command	Description
		show ip ospf

Platform N/A
Description

2.72 timers spf

Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations. Use the **no** form of this command to restore the default setting.

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter Description	Parameter	Description
		<i>spf-delay</i>
	<i>spf-holdtime</i>	Defines the interval between two SPF calculations in seconds. The range is from 0 to 2147483647. When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.

Defaults For the RGOS not supporting the timers throttle spf command, the default values are as follows:

spf-delay: 5seconds;

spf-holdtime: 10 seconds.

For the RGOS supporting the timers throttle spf command, by default, the timers spf command takes no effect. Spf-delay depends on the default configuration of the timers throttle spf command.

Command

Mode Routing process configuration mode

Usage Guide Smaller values of *spf-delay* and *spf-holdtime* mean that OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the router.

 The configurations of the **timers spf command** and the timers throttle spf command may overwrite each other.

Configuration Examples The following example configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.


```
Ruijie(config)# deviceospf20
Ruijie(config-router)# timersspf 3 9
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf.
timers throttle spf	Configures the exponential back off delay for SPF calculation. The command is recommended to replace the timers spf command because it is more powerful.

Platform N/A

Description

2.73 timers throttle lsa all

Use this command to configure the exponential back off algorithm for the LSA. Use the **no** form of this command to restore the default setting.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

Parameter	Description
<i>delay-time</i>	Configures the time delay of generating the LSA first. The range is from 1 to 600000.
<i>hold-time</i>	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is from 1 to 600000.
<i>max-wait-time</i>	Configures the maximum interval of successive refreshing the LSA., which determines whether the LSA is refreshed successively. The range is from 1 to 600000

Defaults

The default configurations are as follows:

Delay-time: 0 millisecond,

Hold-time: 5000 milliseconds,

Max-wait-time: 5000 milliseconds.

Command

Mode Routing process configuration mode

Usage Guide

If high convergence performance is required for the link change, the value of delay-time can be relatively small. if you expect to reduce the CPU consumption, increase appropriately several values.

 The value of hold-time cannot be smaller than that of delay-time, and the value of max-wait-time

cannot be smaller than that of hold-time.

Configuration Examples The following example configures the first delay as 10ms, hold-time as 1second and the longest delay as 5seconds.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf

Platform N/A
Description

2.74 timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default setting.

timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
<i>ia-delay</i>	Sets the delay time of the inter-area route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the <i>ia-delay</i> time runs out.
ase	Calculates the external routes.
<i>ase-delay</i>	Defines the delay time of the external route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the <i>ase-delay</i> time runs out.

Defaults The default values are as follows:
 ia-delay: 0,
 ase-delay: 0,

Command

Mode Routing process configuration mode

Usage Guide The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration The following example sets the .delay time of the inter-area route calculation to one second.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.75 timers throttle spf

Use this command to configure the topology change information for OSPF, including the delay for SPF calculation as well as the interval between two SPF calculations in routing process configuration mode. Use the **no** form of this command to restore the default setting.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
<i>spf-delay</i>	Defines the SPF calculation waiting period, in the unit of milliseconds, in the range from 1 to 600,000. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
<i>spf-holdtime</i>	Defines the interval between two SPF calculations in seconds in the range from 1 to 600,000.
<i>spf-max-waittime</i>	Defines the maximum interval between two SPF calculations, in milliseconds in the range from 1 to 60,000.

Defaults The default configurations are as follows:

spf-delay: 1000ms;

spf-holdtime: 5000ms;

spf-max-waittime: 10000ms.

Command

Mode Routing process configuration mode

Usage Guide The *spf-delay* parameter indicates the delay time of the topology change to the SPF calculation. The *spf-holdtime* parameter indicates the minimum interval between two SPF calculations. Then, the

interval of the consecutive SPF calculations is at least twice as the last interval until it reaches to `spf-max-waittime`. If the interval between two SPF calculations has exceeded the required value, the SPF calculation will restart from `spf-holdtime`.

Smaller `spf-delay` and `spf-holdtime` values can make the topology converge faster. A greater `spf-max-waittime` value can reduce the system resource consumption of SPF calculation. Those configurations can be flexibly adjusted according to the actual stability of the network topology. Compared with the `timers spf` command, this command is more flexible. It speeds up the SPF calculation convergence, and reduces the system resource consumption of SPF calculation due to the topology change. To this end, the `timers throttle spf` command is recommended.

- i The value of `spf-holdtime` cannot be smaller than the value of `spf-delay`, or the value of `ospf-holdtime` will be set to be equal to the value of `spf-delay`;
- The value of `spf-max-waittime` cannot be smaller than the value of `spf-holdtime`, or the value of `spf-max-waittime` will be set to be equal to the value of `spf-holdtime` automatically;
- The configurations of the `timers spf` command and the `timers throttle spf` command may overwrite each other.
- If both the `timers spf` command and the `timers throttle spf` command are not configured, the default value of the `timers throttle spf` command is used.

Configuration Examples The following example configures the delay and holdtime and the maximum time interval of the OSPF as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculation intervals are: 5ms, 1second, 3 seconds, 7 seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90seconds...

```
Ruijie(config)# routerospf20
Ruijie(config-router)# timersspf 5 1000 90000
```

Related Commands

Command	Description
<code>show ip ospf</code>	Displays the configuration information of OSPF
<code>timers spf</code>	Configures the SPF calculation delay. This command is supported in versions earlier than RGOS 10.4. It is recommended to replace the <code>timers spf</code> command with the <code>timers throttle spf</code> command.

Platform N/A

Description

2.76 two-way-maintain

Use this command to enable the OSPF `two-way-maintain` function. Use the **no** form of this command to disable this function.

two-way-maintain

no two-way-maintain

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command

Mode Routing process configuration mode

Usage Guide In the large-scale network, partial packets delay or dropped may exist due to much CPU and memory are occupied caused by lots of packet transmission. If the Hello packets are handled over dead-interval, the corresponding adjacency will be disconnected. In this case, you can enable the two-way-maintain function for the packets such as DD, LSU, LSR and LSAck packets from a neighbor in the network (except for the Hello packets), avoiding the neighbor invalidation caused by delayed or dropped Hello packets.

Configuration The following example disables the OSPF two-way-maintain function.

Examples

```
Ruijie(config)# routerospf1
Ruijie(config-router)# notwo-way-maintain
```

Related Commands	Command	Description
	show ip ospf	Displays the configuration information of the OSPF

Platform N/A
Description

3 OSPFv3 Commands

3.1 area authentication

Use this command to configure OSPFv3 area authentication. Use the **no** form of this command to restore the default setting.

area *area-id* **authentication ipsec spi** *spi* [**md5** | **sha1**] [**0** | **7**] *key*
no area *area-id* **authentication**

Parameter Description	Parameter	Description
	<i>area-id</i>	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
	<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
	md5	Specifies a message digest 5 (MD5) authentication mode.
	sha1	Specifies a secure hash algorithm 1 (SHA1) authentication mode.
	0	Indicates that a key is displayed in a plain-text format.
	7	Indicates that a key is displayed in a cipher-text format.
	<i>key</i>	Specifies an authentication key.

Defaults Authentication is not performed by default.

Command Mode Routing process configuration mode

Usage Guide RGOS supports three authentication modes:

- null authentication mode, which is configured when authentication is not needed
- MD5 authentication mode
- SHA1 authentication mode

If OSPFv3 area authentication is configured, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Interface authentication configuration, however, takes precedence over area authentication configuration.

Configuration Examples The following example specifies MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-router)# area 1 authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands	Command	Description
------------------	---------	-------------

ipv6 ospf authentication	Specifies interface authentication.
area virtual-link authentication	Specifies virtual link authentication.

Platform N/A

Description

3.2 area default-cost

Use this command to set the cost of the default route for the ABR in the stub or NSSA area. Use the **no** form of this command to restore the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **authentication**

Parameter Description	Parameter	Description
	<i>area-id</i>	Area ID of the stub or NSSA area. It can be an integer or an IPv4 prefix.
	<i>cost</i>	Cost of the default route of the stub or NSSA area in the range from 0 to 16777215.

Defaults The default cost is 1.

Command Mode Routing process configuration mode.

Usage Guide This command can only work in the ABR connected to the stub area.

Configuration Examples The following example sets the cost of the default route of stub area 50 to 100.

```

ipv6 router ospf 1
area 50 stub
area 50 default-cost 100

```

Related Commands	Command	Description
	area stub	Sets a stub area.

Platform N/A

Description

3.3 area encryption

Use this command to enable encryption authentication for an OSPFv3 area. Use the **no** form of this command to restore the default setting.

```
area area-id encryption ipsec spi spi esp null [ md5 | sha1 ] [ 0 | 7 ] key
no area area-id encryption
```

**Parameter
Description**

Parameter	Description
<i>area-id</i>	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
<i>Key</i>	Specifies an authentication key.

Defaults Encryption authentication is not performed by default.

**Command
Mode** Routing process configuration mode

Usage Guide RGOS supports the null encryption mode and two authentication modes: MD5 and SHA1. If encryption authentication is configured for an OSPFv3 area, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Encryption authentication configuration on interfaces, however, takes precedence over that of the OSPFv3 area.

**Configuration
Examples** The following example specifies null encryption and MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaa.
Ruijie(config-router)# area 1 encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

**Related
Commands**

Command	Description
ipv6 ospf encryption	Specifies interface encryption authentication.
area virtual-link encryption	Specifies virtual link encryption authentication.

**Platform
Description** N/A

3.4 area nssa

Use this command to configure an NSSA area. Use the **no** form of this command to remove the

NSSA area configuration.

```
area area-id nssa [ no-redistribution ] [ default-information-originate [ metric value ]
[ metric-type type ] ] [ no-summary ] [ translator [ stability-interval seconds | always ] ]
no area area-id nssa [ no-redistribution ] [ default-information-originate [ metric ] [ metric-type ] ]
[ no-summary ] [ translator [ stability-interval | always ] ]
```

**Parameter
Description**

Parameter	Description
<i>area-id</i>	ID of the NSSA area.
no-redistribution	(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal areas, but not into the NSSA area.
default-information-originate	(Optional) Used to generate a Type 7 default into the NSSA area. This keyword takes effect only on the NSSA ABR or the NSSA Autonomous System Boundary Router (ASBR).
metric <i>value</i>	(Optional) Specifies the OSPF default LSA metric. The range is from 0 to 16,777,214, and the default value is 1.
metric-type <i>type</i>	(Optional) Specifies the OSPF metric type for default routes. The value can be 1 or 2 and the default value is 2.
no-summary	(Optional) Allows an area to be an NSSA but not have summary routes injected into it.
translator	(Optional) Configures the NSSA ABR translator.
stability-interval <i>seconds</i>	(Optional) Configures the stability interval after the role of an NSSA ABR is changed from translator to non-translator. The range is from 0 to 2,147,483,647, the default value is 40 and the unit is second.
always	(Optional) Configures the NSSA ABR to be always translator. The default NSSA ABR is a non-translator.

Defaults No NSSA area is defined by default.

Command

Mode Routing process configuration mode

Usage Guide

The **default-information-originate** parameter is used to generate a default Type 7 LSA. There is a small difference between NSSA ABR and NSSA ASBR on which this command can take effect. On the ABR, the Type-7 default route generates no matter whether a default route exists in the routing table, while on the ASBR, the Type-7 default route generates only when a default routes exists in the routing table.

The **no-redistribution** parameter is used when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal areas, but not into the NSSA area. This parameter is generally used on the device acting as both ASBR and ABR in NSSA area to prevent the routes from being imported into the NSSA area.

The **no-summary** parameter allows an area to be an NSSA but not have summary LSAs injected into

it.

In an NSSA area involving two or more ABR devices, by default, the ABR of larger router ID is elected as the translator for Type-7 to Type-5 translation. You can configure the **translator always** parameter to specify an ABR to be always the translator.

When the translator of an ABR device is replaced, the ABR still has the translation capability within the **stability-interval** time. After the stability-interval timer expires and the ABR is not elected as the translator again, then the LSAs translated from Type-7 to Type-5 will be removed from the AS.

To prevent route loop, the Type-5 LSAs aggregated by the Type-7 are removed once the ABR device loses the translator capability, instead of waiting for the stability-interval expiration.

It is recommended to configure the **translator always** parameter on only one ABR device in an NSSA area.

Configuration The following example sets the area 1 as an NSSA area.

Examples

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# area 1 nssa
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

3.5 area-range

Use this command to set the range of the converged inter-area addresses. Use the **no** form of this command to restore the default setting.

area *area-id* **range** *ipv6-prefix/prefix-length* [**advertise**|**not-advertise**]

no area *area-id* **range** *ipv6-prefix/prefix-length*

**Parameter
Description**

Parameter	Description
<i>area-id</i>	ID of the area in which the addresses are converged. It can be an integer or an IPv4 prefix.
<i>ipv6-prefix/prefix-length</i>	Range of the converged addresses.
advertise	Advertises the range of converged addresses.
not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.

Defaults No converged inter-area address range is defined by default.

**Command
Mode** Routing process configuration mode

Usage Guide This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. The routing information combination only takes place on the area border. The specific routing information is seen on the intra-area routers, but only one converged route can be seen on the devices in other areas. By configuring the two options of advertise and not-advertise, you can decide whether to advertise the convergence range to enable blocking and filtering. By default, the range is advertised to the outside. The option cost can be used to set the metric value of convergence routing.

A number of route convergence commands can be defined. In this way, the number of the routes in the OSPF AS is reduced. Particularly for a large network, the forwarding performance will be improved.

When a number of routes are converged, and the containment relationship exists between items, the area range converged is determined by the longest match principle.

Configuration The following example converges the routes in area 1.

Examples

```
ipv6 router ospf 1
area 1 range 2001:abcd:1:2::/64
```

**Related
Commands**

Command	Description
summary-prefix	Sets the range of the external routes to be converged.

Platform N/A
Description

3.6 area stub

Use this command to create a stub area or set its attributes. Use the **no** form of this command to restore the default setting.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

**Parameter
Description**

Parameter	Description
<i>area-id</i>	ID of the stub area. It can be an integer or an IPv6 prefix.
no-summary	This option applies only to the ABR in the stub area, indicating that the ABR only advertises the type 3 LSA indicating the default route to the stub area, not other type 3 LSAs.

Defaults No stub area is defined by default.

Command Routing process configuration mode

Mode

Usage Guide If an area is at the end of an entire network, it can be designed as the stub area, in which all the routers must execute the `area stub` command. If the area is designed as the stub area, it cannot learn the AS external routing information (type 5 LSAs). In practical application, the external routing information takes a large proportion of the link state database, so the devices in the stub area can only learn very little routing information, thus reducing the system resources required for the running of the OSPFv3 protocol.

By default, a type 3 LSA advertisement indicating default routing on the ABR in the stub area is generated, then the devices in the stub area can get to the outside of the AS.

If a totally stub area needs to be configured, just select the keyword **no-summary** when executing the `area stub` command on the ABR.

Configuration The following example enables the ABR in stub area 10 to advertise the default route to the stub area.

Examples

```
ipv6 router ospf 1
area 10 stub
area 10 stub no-summary
```

Related Commands

Command	Description
<code>area default-cost</code>	Sets the cost of the default route in the stub area.

Platform N/A

Description

3.7 area virtual-link




Use this command to create a virtual link or set its parameters. Use the **no** form of this command to restore the default setting.

```
area area-id virtual-link router-id [ hello-interval seconds ] [ dead-interval seconds ]
[ retransmit-interval seconds ] [ transmit-delay seconds ] [ instance instance-id ] [ authentication
ipsec spi spi [ md5 | sha1 ] [ 0 | 7 ] key ] [ encryption ipsec spi spi esp null [ md5 | sha1 ] [ 0 | 7 ]
key ]
```

```
no area area-id virtual-link router-id [ hello-interval ] [ dead-interval ] [ retransmit-interval ]
[ transmit-delay ] [ instance ] [ authentication ] [ encryption ]
```

Parameter Description

Parameter	Description
<i>area-id</i>	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
<i>Router-id</i>	Neighbor router ID of the virtual link.
hello-interval <i>seconds</i>	Sets the interval to send the hello message on the local virtual link interface in the range from 1 to 65535 in the unit of seconds.



dead-interval <i>seconds</i>	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. It is in the range from 1 to 65535 in the unit of seconds.
retransmit-interval <i>seconds</i>	Interval for retransmitting LSA on the local interface of the virtual link . The range is from 1 to 65535 in the unit of seconds.
transmit-delay <i>seconds</i>	Delay on the local interface of the virtual link in sending LSA. The range is from 1 to 65535 in the unit of seconds.
instnace <i>instance-id</i>	Specifies the instance corresponding to the virtual link. No virtual link can be established between different instances. Range: 0.-255
authentication ipsec spi <i>spi [md5 sha1] [0 7] key</i>	Specifies OSPFv3 authentication.  Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format. <i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295. md5 specifies the MD5 authentication mode. sha1 specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. <i>key</i> specifies an authentication key.
encryption ipsec spi spi esp null [md5 sha1] [0 7] <i>key</i>	Specifies OSPFv3 encryption authentication.  Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format. <i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295. null specifies the null encryption mode. md5 specifies the MD5 authentication mode. sha1 specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. <i>key</i> specifies an authentication key.
authentication ipsec spi <i>spi [md5 sha1] [0 7] key</i>	Specifies OSPFv3 authentication.  Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format. <i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295. md5 specifies the MD5 authentication mode. sha1 specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format.

<i>key</i> specifies an authentication key.

Defaults No virtual link is defined by default
hello-interval: 10 seconds; dead-interval: four times of the hello-interval; retransmit-interval: five seconds; transmit-interval: one second.
Authentication and encryption are not performed by default.

Command Mode Routing process configuration mode

Usage Guide In the OSPFv3 AS, all the areas must be connected with the backbone area to ensure that they can learn the routes of the whole OSPFv3 AS. If an area cannot be directly connected with the backbone area, it can connect it through a virtual link.

-  The virtual link shall not be in the stub or NSSA area.
-  configuration, **dead-interval** and **instance** shall be configured consistently on both sides of the virtual link neighbors, otherwise neighboring relationship cannot be set up between the virtual neighbors.

Configuration The following example configures a virtual link.

Examples

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# area 1 virtual-link 192.1.1.1
```

Related Commands

Command	Description
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
show ipv6 ospf virtual-links	Displays the OSPFv3 virtual link information.

Platform N/A
Description

3.8 auto-cost

The metric of the OSPFv3 protocol is the interface-based bandwidth. Use this command to enable the bandwidth-based interface metric calculation or modify the reference bandwidth. Use the **no** form of this command to restore the default setting.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
-----------	-------------

reference-bandwidth <i>ref-bw</i>	Reference bandwidth in the range from 1 to 4294967 Mbps.
---	--

Defaults The interface metric is calculated based on the reference bandwidth, which is 100Mbps.

Command Mode Routing process configuration mode

Usage Guide Use **no auto-cost reference-bandwidth** to restore it to the default reference bandwidth. You can use **ipv6 ospf cost** in the interface configuration mode to set the cost of the specified interface, and it takes precedence over the metric calculated based on the reference bandwidth.

Configuration Examples The following example changes the reference bandwidth to 10M.

```
ipv6 router ospf 1
auto-cost reference-bandwidth 5
```

Related Commands

Command	Description
ipv6 ospf cost	Sets the cost of an interface.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

3.9 bdf all-interfaces

Use this command to enable the BDF on all OSPFv3 interfaces. Use this command to enable the BDF on all OSPFv3 interfaces in the routing configuration mode. Use the **no** form of this command to restore the default setting.

bdf all-interfaces

no bdf all-interfaces

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Routing process configuration mode.

Usage Guide The OSPFv3 protocol dynamically discovers the neighbors through the Hello packets. With the BFD function enabled, BFD sessions will be established for the neighbors that match the FULL rules and

the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPFv3 will perform the network convergence immediately.

You can also use the interface configuration mode command **ipv6 ospf bfd [disable]** to enable or disable the BFD function on the specified interface, which takes precedence over the command **bfd all-interfaces** in the routing process configuration mode.

Configuration N/A

Examples

Related Commands

Command	Description
ipv6 router ospf <i>process-id</i>	Enables the OSPFv3 routing process and enter into the routing process configuration mode.
ipv6 ospf bfd [disable]	Enables or disable the BFD on the specified OSPFv3 interfaces.

Platform N/A

Description

3.10 clear ipv6 ospf process

Use this command to clear and restart the OSPF process.

clear ipv6 ospf { process | process-id }

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID, in the range from 1 to 65535

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

In normal case, it is not necessary to use this command.

Use the parameter *process-id* to clear only one specific OSPFv3 instance. If no *process-id* is specified, all the OSPFv3 instances will be cleared.

Configuration The following example restarts the OSPF process.

Examples

```
enable
clear ipv6 ospf process
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

3.11 default-information originate

Use this command to generate a default route to the OSPFv3 routing domain in the routing process mode. Use the **no** form of this command to restore the default setting.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

Parameter Description	Parameter	Description
	always	(Optional) It makes OSPFv3 generate the default route unconditionally, no matter whether the default route exists locally or not.
	metric <i>metric</i>	(Optional) Initial metric value of the default route, in the range from 0 to 16777214
	metric-type <i>type</i>	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric seen on different routers.
	route-map <i>map-name</i>	Associated route-map name, no associated route-map by default

Defaults No default route is created;
The initial metric value is 1;
The default route type is type 2.

Command Mode Routing process configuration mode

Usage Guide When the **redistribute** or **default-information** command is executed, the OSPFv3-enabled router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate the default route automatically or advertise it to all the routers in the OSPFv3 routing domain. The ASBR generates default routes by default. It is required to configure with the routing process configuration command **default-information originate**.

If the **always** parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route in the core routing table exists or not. However, the local router does not display the default route. To make sure whether the default route is generated, execute **show ipv6 ospf database** to observe the OSPF link state database. The execution of the **show ipv6 route** command on the OSPF neighbor will display the default route.

The metric of the external default route can be defined only with the **default-information originate** command and cannot be set with the **default-metric** command.

There are two types of OSPFv3 external routes: type 1 external routes have changeable routing

metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the **show ipv6 route** command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area. To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

Configuration The following example generates a default route.

Examples

```
default-information originate always
```

**Related
Commands**

Command	Description
redistribute	Redistribute routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

Platform N/A

Description

3.12 default-metric

Use this command to set the default metric for the routes to be redistributed. Use the **no** form of this command to restore the default setting

default-metric *metric-value*

no default-metric

**Parameter
Description**

Parameter	Description
<i>metric-value</i>	Default metric for the routes to be redistributed. Its range is from 1 to 16777214.

Defaults The default is 20.

Command

Mode The default route type is type 2.

Usage Guide This command can be used together with **redistribute** to set the default metric for the routes to be redistributed. But this command does not apply to two types of routes:

- The **default route generated** with default-information originate;
- The redistributed direct route, for which 20 is always the default metric value.

Configuration The following example sets the default metric for the routes to be redistributed to 10.

Examples

```
default-metric 10
```

**Related
Commands**

Command	Description
redistribute	Redistributes the routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform N/A

Description

3.13 distance

Use this command to set the management distance corresponding to different types of OSPFv3 routes. Use the **no** form of this command to restore the default setting.

distance { *distance* | **ospf** { **intra-area** *distance* | **inter-area** *distance* | **external** *distance* } }

no distance [**ospf**]

**Parameter
Description**

Parameter	Description
<i>distance</i>	Sets the management distance of the route, in the range from 1 to 255.
intra-area <i>distance</i>	Sets the management distance of the intra-area route, in the range from 1 to 255.
inter-area <i>distance</i>	Sets the management distance of the inter-area route, in the range from 1 to 255.
external <i>distance</i>	Sets the management distance of the external route, in the range from 1 to 255.

Defaults

The default value is 110.

Management distance of the intra-area route :110,

Management distance of the inter-area route :110


Management distance of the external-area route: 110.


**Command
Mode**

Routing process configuration mode.

Usage Guide

This command is used to specify different management distances for different types of OSPFv3 routes. The management distance of the route is used for the comparison of routing priority, the smaller the management distance is, the higher the routing priority.

 The priority of the route generated by different OSPFv3 processes must be compared using the management distance.

 Setting the management distance as 255 indicates the routing entry is unreliable and will not for the packet forwarding.

Configuration the following example sets the OSPFv3 external route management distance to 160.

Examples

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# distance ospf external 160
```

Related Commands

Command	Description
ipv6 router ospf	Enables the OSPFv3 routing process .

Platform

N/A

Description

3.14 distribute-list in

Use this command to filter routes that are computed based on Link State Advertisement (LSA). Use the **no** form of this command to restore the default setting.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type* *interface-number*]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type* *interface-number*]

Parameter Description

Parameter	Description
<i>name</i>	Specifies an ACL filtering rule.
prefix-list <i>prefix-list-name</i>	Specifies a prefix list filtering rule.
<i>interface-type</i> <i>interface-number</i>	Specifies an interface on which LSA-based routes are filtered.

Defaults

Routes are not filtered by default.

Command Mode

Routing process configuration mode

Usage Guide

Filter the routes computed based on LSA. Only the routes meeting filtering conditions can be forwarded. Route filtering does not affect the link state database and the routing tables of the neighbors. The ACL and prefix list filtering rules cannot be set at the same time. You can set only the ACL filtering rule or the prefix list filtering rule for a specific interface.

The routing filtering rules affect only forwarding of local routes but not route computation based on LSA. When route filtering is configured on an ABR, LSA can still compute routes and generate and send inter-area LSAs with prefixes to other areas. This will cause blackhole routes. To prevent the generation of blackhole routes, you can run the **area range** command with the **not-advertise** keyword.

Configuration The following example filters routes that are computed based on Link State Advertisement (LSA).

```
Ruijie(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64
Ruijie(config)# ipv6 router ospf 25
Ruijie(config-router)# redistribute rip metric 100
Ruijie(config-router)# distribute-list prefix-list aaa in ethernet 0/1
```

**Related
Commands**

Command	Description
area range	Configures route aggregation in an area.

Platform N/A

Description

3.15 distribute-list out

Use this command to filter routes that are re-distributed. This command has the similar function as the **redistribute** command. Use the **no** form of this command to restore the default setting.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

**Parameter
Description**

Parameter	Description
<i>name</i>	Specifies the ACL filtering rule.
prefix-list <i>prefix-list-name</i>	Specifies the prefix list filtering rule.
bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static	Specifies the source from which the routes are filtered.

Defaults Routes are not filtered by default.

**Command
Mode** Routing process configuration mode

Usage Guide The **distribute-list out** command has the similar function as the **redistribute route-map** command. It can be used to filter the routes that are re-distributed based on other protocols into an OSPFv3 area. It does not directly re-distribute routes but works with the **redistribute** command to re-distribute routes. The ACL and prefix list filtering rules cannot be configured at the same time. You can set only the ACL filtering rule or the prefix list filtering rule to filter the routes from a specific source.

Configuration The following example filters static routes that are re-distributed.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# redistribute static subnets
```

```
Ruijie(config-router)# distribute-list prefix-list jjj out static
```

**Related
Commands**

Command	Description
redistribute	Re-distributes routes that are carried by other routing processes.

Platform N/A

Description

3.16 enable mib-binding

Use this command to bind MIB to a specific OSPFv3 process. Use the **no** form of this command to restore the default setting.

enable mib-binding

no enable mib-binding

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

MIB is bound to an OSPFv3 process with the smallest process number by default.

**Command
Mode**

Routing process configuration mode

Usage Guide

OSPFv3 MIB has no configuration information about OSFPv3 processes. You can operate only one OSFPv3 process through SNMP. OSFPv3 MIB is bound to the OSFPv3 process with the smallest process number by default. Users' operations take effect on this process.

To operate a specific OSFPv3 process through SNMP, you can bind OSFPv3 MIB to the process.

Configuration

The following example enables users to operate the OSPFv3 process with the process number of 100 through SNMP.

Examples

```
Ruijie(config)# ipv6 router ospf 100
Ruijie(config-router)# enable mib-binding
```

**Related
Commands**

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable traps	Enables the OSPFv3 trap function.

Platform N/A

Description

3.17 enable traps

OSPFv3 processes support eight types of trap information, which are classified into two categories. Use this command to send specific trap information. Use the **no** form of this command to restore the default setting.

enable traps [**error** [**IfConfigError** | **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **state-change** [**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** | **VirtNbrStateChange**]]

no enable traps [**error** [**IfConfigError** | **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **state-change** [**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** | **VirtNbrStateChange**]]

Parameter Description

Parameter	Description
Error	Configures all error-related trap types. This keyword can also specify the following types of error traps:
	IfConfigError Specifies an interface parameter error;
	IfRxBadPacket Specifies incorrect packets received by an interface;
	VirtIfConfigError Specifies a parameter error on a virtual interface;
VirtIfRxBadPacket Specifies incorrect packets received by a virtual interface.	
state-change	Configures all traps related to state change. This keyword can also specify the following traps related to state change:
	IfStateChange Specifies state change of an interface;
	NbrStateChange Specifies state change of a neighbor;
	NssaTranslatorStatusChange Specifies status change of the NSSA translator.
	VirtIfStateChange Specifies state change of a virtual interface;
VirtNbrStateChange Specifies state change of a virtual neighbor.	

Defaults All traps are disabled by default.

Command Mode Routing process configuration mode

Usage Guide Before configuring this command, you must run the **snmp-server enable traps ospf** command; otherwise, OSPFv3 trap information cannot be sent correctly. This is because the function of this

command is restricted by the **snmp-server** command.

You can synchronously enable the trap function of different processes even if MIB is not bound to these processes.

Configuration The following example enables all traps of OSPFv3 process 100.

Examples

```
Ruijie(config)#ipv6 router ospf 100
Ruijie(config-router)# enable traps
```

**Related
Commands**

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable mib-binding	Binds MIB to an OSPFv3 process.
snmp-server enable traps ospf	Enables OSPFv3 to send trap information.

Platform N/A

Description

3.18 graceful-restart

Use this command to enable the OSPFv3 graceful restart (GR) function and to set the GR period.

Use the **no** form of this command to restore the default setting.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [*graceful-period*]

**Parameter
Description**

Parameter	Description
grace-period <i>grace-period</i>	Configures the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment when OSPFv3 gracefully restarts. The GR period is in the range from 1 to 1800 in the unit of seconds. The default is 120.
inconsistent-lsa-checking	Configures the topology change detection. Once the topology change is detected, the device will exit GR and finish the convergence, This function is enabled by default after GR is enabled.

Defaults This function is enabled by default.

Command

Mode Routing process configuration mode

Usage Guide GR is configured based on the OSPFv3 instance. Different instances could be configured with different parameters.

Use this command to configure the GR period. The GR period is the longest interval that lasts from

the moment when OSPFv3 fails to the moment that OSPFv3 gracefully restarts. In this period, the device will perform link reconstruction to restore OSPFv3. When the GR period expires, OSPFv3 exits GR and finishes regular operation.

To enable the GR function and set the GR period to the 120 seconds, use the **graceful-restart** command. To modify the GR period, use the **graceful-restart grace-period** command. Topology stability is indispensable for uninterrupted forwarding. If topology changes, OSPFv3 finishes convergence instead of continuing GR to avoid long time interruption

1) Disabling the topology change detection: If the topology cannot converge in time in the hot backup process, the long term forwarding interruption may occur.

2) Enabling the topology change detection: Forwarding interruption may occur but the interruption time is much shorter than the time it takes to disable topology detection.

It is not recommended to disable the topology change detection. In some scenario where long term forwarding interruption does not occur, disabling the topology change detection minimizes the forwarding interruption time.

The GR function is unavailable when the Fast Hello function is enabled.

Configuration The following example enables GR for OSPFv3 instance 1 and sets the GR period to 60 seconds.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# graceful-restart
Ruijie(config-router)# graceful-restart grace-period 60
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.19 graceful-restart helper

Use this command to enable the OSPFv3 graceful restart helper function. Use the **no** form of this command to disable this function.

graceful-restart helper disable

no graceful-restart helper disable

Use this command configure the topology change detection method of OSPFv3 GR helper. Use the **no** form of this command to cancel the configuration.

graceful-restart helper { strict-lsa-checking | internal-lsa-checking }

no graceful-restart helper { strict-lsa-checking | internal-lsa-checking }

**Parameter
Description**

Parameter	Description
disable	Disables the device to assist other devices in performing GR.
strict-lsa-checking	Checks the change of the LSA of types 1-5 and 7 to judge whether the network topology changes. If the topology changes, the GR

	helper function will be disabled.
internal-lsa-checking	Checks the change of the LSA of types 1–3 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.

Defaults The GR helper is enabled by default.
The device where the GR helper is enabled does not check the LSA change by default.

Command

Mode Routing process configuration mode

Usage Guide Use this command to enable the GR helper function. When one neighbor device performs graceful restart, the Grace-LSA is advertised to all neighbors. If the device enabled with the GR helper receives the Grace-LSA, it will become the GR Helper to help the neighbors perform GR. The **disable** option means that it is not allowed to perform the GR helper function for any device in GR. The GR helper does not perform the network change detection by default. The convergence is not performed again until the GR is implemented even if the network changes. Use the **strict-lsa-checking** or **internal-lsa-checking** command to enable the device to detect the change of network topology during the GR. The former checks any LSA (types 1-5,7) that stands for the network information, the latter checks the LSA that stands for the AS inner-area route. In the large scale network, it is not recommended to enable the LSA check option because the partial network changes trigger the ending of the GR, decreasing the convergence speed of the entire network.

Configuration Examples The following example disables the GF helper function of the OSPFv3 instance 1 and modifies the topology change detection policy.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# graceful-restart helper disable
Ruijie(config-router)# no graceful-restart helper disable
Ruijie(config-router)# graceful-restart helper strict-lsa-checking
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

3.20 ipv6 ospf area

Use this command to enable the interface to participate in the OSPFv3 routing process. Use the **no** form of this command to restore the default setting.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID.
	area <i>area-id</i>	OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide You can use this command to enable the OSPFv3 on an interface, and then configure the OSPFv3 process with **ipv6 router ospf**. It will be automatically started after this command is used., it will be automatically started after this command is used.

Use **no ipv6 ospf area** to disable the specified interface to participate in the OSPFv3 routing process.

Use **no ipv6 router ospf** to disable all the interfaces to participate in the OSPFv3 routing process.

The neighbor relationship can only be established between the routers with the same instance ID.

After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3.

Configuration Examples The following example starts the OSPFv3 process on int fastethernet 0/0 for the specified area of the specified instance.

```
int fastethernet 0/0
ipv6 ospf 1 area 2 instance 2
```

Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	passive-interface	Setsthe a passive interface.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform N/A

Description

3.21 ipv6 ospf authentication

Use this command to configure OSPFv3 interface authentication. Use the **no** form of this command to restore the default setting.

ipv6 ospf authentication [null | ipsec spi *spi* [md5 | sha1] [0 | 7] *key*]
no ipv6 ospf authentication

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
null	Indicates that authentication is not performed.
<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
<i>key</i>	Specifies an authentication key.

Defaults Authentication is not performed by default.

Command Mode Interface configuration mode

Usage Guide RGOS supports three authentication modes:

- null authentication mode, which is configured when authentication is not needed
- MD5 authentication mode
- SHA1 authentication mode

 OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.

Configuration Examples The following example specifies MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-if)# ipv6 ospf authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands	Command	Description
	ipv6 ospf authentication	Specifies interface authentication.
	area virtual-link authentication	Specifies virtual link authentication.

Platform Description N/A

3.22 ipv6 ospf bfd

Use this command to enable or disable the BFD on the specified OSPFv3-enabled interface. Use the **no** form of this command to restore the default setting.

```
ipv6 ospf bfd [ disable ] [ instance instance-id ]
no ipv6 ospf bfd [ instance instance-id ]
```

Parameter Description	Parameter	Description

disable	Disables the BFD function on the specified OSPF interface.
instance <i>instance-id</i>	Configures the specified OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults No configuration is made by default. The BFD configuration in the OSPFv3 process configuration mode will apply.

Command

Mode Interface configuration mode.

Usage Guide The command `ipv6 ospf bfd` in the interface configuration mode takes precedence over the **bfd all-interfaces** command in the routing process configuration mode. You can use this command to enable the BFD on the specified interface according to the actual environment, also can use the command **bfd all-interfaces** in the OSPFv3 process configuration mode to enable the BFD function on all OSPFv3 interfaces and use the command `ip v6 ospf bfd disable` to disable the BFD on the specified interface.

Configuration Ruijie(config)# int fastethernet 0/0
Examples Ruijie(config-if-fastethernet 0/0)# ipv6 ospf bfd

Related Commands

Command	Description
ipv6 router ospf <i>process-id</i>	Starts the OSPFv3 routing process and enter into the routing process configuration mode.
bfd all-interfaces	Enables the BFD on all OSPFv3 interfaces.

Platform N/A

Description

3.23 ipv6 ospf cost

Use this command to set the cost of the interface. Use the **no** form of this command to restore the default setting

ipv6 ospf cost *cost* [**instance** *instance-id*]

no ipv6 ospf cost [**instance** *instance-id*]

Parameter Description

Parameter	Description
<i>Cost</i>	Cost of interface, in the range from 0 to 65535.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults The default interface cost is the reference bandwidth/Bandwidth (100Mbps by default).

Command Mode	Interface configuration mode.
Usage Guide	<p>By default, the cost of the OSPFv3 interface is 100Mbps/Bandwidth, in which the Bandwidth is the bandwidth of the interface and configured with the command bandwidth in the interface configuration mode.</p> <p>The default costs of OSPFv3 interfaces for several typical lines are:</p> <ul style="list-style-type: none"> ● 64K serial line: 1562; ● E1 line: 48 ● 10M Ethernet: 10 ● 100M Ethernet: 1 <p>The OSPFv3 cost configured with the command ipv6 ospf cost will overwrite the default configuration.</p>

Configuration The following example sets the cost of the interface to 1:

Examples

```
Ruijie(config)# int fastethernet 0/0
Ruijie(config-if)# ipv6 ospf cost 1
```

Related Commands	Command	Description
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform N/A

Description

3.24 ipv6 ospf dead-interval

Use this command to set a dead interval of neighbors on an interface. If no hello packet is received from a neighbor within the interval, the neighboring relationship is considered to fail. Use the **no** form of this command to restore the default setting

ipv6 ospf dead-interval { *seconds* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]
no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter Description	Parameter	Description
	<i>seconds</i>	Dead interval of neighbors. Its range is from 1 to 65535 in the unit of seconds.
	minimal hello-multiplier <i>multiplier</i>	Enables the fast hello function, which takes 1s as the dead interval of neighbors. <i>Multiplier</i> specifies the number of hello packets sent in one second, in the range from 3 to 20.

instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.
------------------------------------	---

Defaults If the fast hello function is not enabled, the dead interval of neighbors is four times longer than the hello interval.


 If the hello interval is changed, the dead interval of neighbors varies automatically.

Command Mode Interface configuration mode

Usage Guide The dead interval of neighbors must be longer than the hello interval.

The OSPFv3 fast hello function allows OSPFv3 to fast discovery neighbors and detect whether neighboring relationships are valid. To enable the OSPFv3 fast hello function, you can specify the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter in this command. **minimal** specifies the deal interval of neighbors to be 1s; **hello-multiplier** specifies the number of times that hello packets are sent in a second. Therefore, this configuration reduces the hello interval to be shorter than 1s.

If an interface is enabled with the fast hello function, the **hello-interval** field of hello packets to be advertised by this interface is set to 0, and that of hello packets received from this interface is omitted.

 **dead-interval**, **minimal**, and **hello-multiplier** that are introduced to enable the fast hello function cannot be configured together with **hello-interval**.

No matter whether the fast hello function is configured, the dead interval of neighbors on the interconnected interfaces of neighbors must be consistent. The values of **hello-multiplier** on the interconnected interfaces can be different but you must ensure that at least one hello packet is received within the dead interval of neighbors.

You can use the **show ipv6 ospf interface** command to monitor the dead interval of neighbors and the fast hello interval on an interface.

Configuration Examples The following example sets the dead interval of neighbors to 60 seconds on an interface.

```
ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
ipv6 ospf hello-interval	Sets the interval for sending the Hello message on an interface.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process

Platform Description N/A

3.25 ipv6 ospf encryption

Use this command to enable OSPFv3 encryption authentication on an interface. Use the **no** form of this command to restore the default setting.

ipv6 ospf encryption [**null** | **ipsec spi spi esp null** [**md5** | **sha1**] [**0** | **7**] *key*]

no ipv6 ospf encryption

Parameter Description

Parameter	Description
null	Indicates that encryption authentication is not performed.
<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
<i>key</i>	Specifies an authentication key.

Defaults


Encryption authentication is not performed by default.

Command Mode

Interface configuration mode

Usage Guide

RGOS supports the null encryption mode and two authentication modes: MD5 and SHA1.

 OSPFv3 encryption authentication parameters configured on interconnected interfaces must be consistent.

Configuration Examples

The following example specifies null encryption and MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-if)# ipv6 ospf encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
area encryption	Specifies area encryption authentication.
area virtual-link encryption	Specifies virtual link encryption authentication.

Platform

N/A

Description

3.26 ipv6 ospf hello-interval

Use this command to set the interval for the interface to send the Hello message. Use the **no** form of this command to restore the default setting

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
<i>seconds</i>	Interval for sending the Hello message. Its range is from 1 to 65535 in the unit of seconds.
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.

Defaults

The broadcast network and point-to-point network :10 seconds. The point-to-multipoint network and NBMA network :30 seconds.

Command

Mode

Interface configuration mode.

Usage Guide

The same hello sending intervals must be set for the neighbors, otherwise the normal adjacency cannot be established.



The dead-interval minimal hello-multiplier and hello-interval parameters for Fast Hello cannot be configured simultaneously.

Configuration

The following example sets the interval for the interface to send the Hello message to 20 seconds.

Examples

```
ipv6 ospf hello-interval 20
```

Related Commands

Command	Description
ipv6 ospf dead-interval	Sets the interval for the interface to consider that the neighbor fails.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform

N/A

Description

3.27 ipv6 ospf mtu-ignore

Use this command to ignore the MTU check when an interface receives the database description message. Use the **no** form of this command to restore the default setting.

```

ipv6 ospf mtu-ignore [ instance instance-id ]
no ipv6 ospf mtu-ignore [ instance instance-id ]

```

**Parameter
Description**

Parameter	Description
instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults The MTU check is enabled by default.

Command

Mode Interface configuration mode.

Usage Guide After receiving the database description message, the OSPFv3 device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an MTU greater than its own interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration The following example disables the MTU check function on the ethernet 1/0.

Examples

```

Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ipv6 ospf mtu-ignore

```

**Related
Commands**

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 mtu	Sets the value of IPv6 MTU of the interface.

Platform N/A

Description

3.28 ipv6 ospf neighbor

Use this command to configure the OSPFv3 neighbor manually. Use the **no** form of this command to restore the default setting.

```

ipv6 ospf neighbor ipv6-address [ [ cost <1-65535> ] [ poll-interval <0-2147483647> | priority <0-255> ] ] [ instance instance-id ]
no ipv6 ospf neighbor ipv6-address [ [ cost <1-65535> ] [ poll-interval < 0-2147483647 > | priority < 0-255 > ] ] [ instance instance-id ]

```

**Parameter
Description**

Parameter	Description
cost <i>cost</i>	(Optional) Configures the cost to each neighbor in point-to-multipoint network. It is not defined by default, where the cost configured on the interface will be used. It ranges from 1 to 65535.

	Only the networks of the point-to-multipoint type support this option.
poll-interval <i>seconds</i>	(Optional) Interval for polling the neighbors (in seconds), which ranges from 1 to 2147483647. Only the networks of the non-broadcast (NBMA) type support this option.
priority <i>priority</i>	(Optional) Configures the priority value of non-broadcast network neighbors, which ranges from 0 to 255. Only the non-broadcast (NBMA) type network supports this option.
instance <i>instance-id</i>	(Optional) Configures the specific OSPFv3 instance on the interface, which ranges from 0 to 255.

Defaults No neighbor is defined;
Neighbor polling interval: 120 seconds;
Priority value of non-broadcast network neighbor: 0.

Command

Mode Interface configuration mode.

Usage Guide You can set relevant parameters for the neighbors depending on the actual network type.

Configuration The following example shows how to configure the OSPFv3 neighbor as follows: IPv6 address:

Examples 2001:DB8:4::1, priority value: 1, polling interval: 150 seconds.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 ospf neighbor 2001:DB8:4::1 priority 1 poll-interval
150
```

**Related
Commands**

Command	Description
ipv6 ospf priority	Sets the priority value of an interface.
ipv6 ospf network	Sets the network type of an interface.

Platform N/A

Description

3.29 ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore the default setting.

```
ipv6 ospf network { broadcast | non-broadcast | point-to-point | point-to-multipoint
[ non-broadcast ] } [ instance instance-id ]
```

```
no ipv6 ospf network [ broadcast | non-broadcast | point-to-point | point-to-multipoint
[ non-broadcast ] ] [ instance instance-id ]
```

Parameter

Parameter	Description
-----------	-------------

Description	
broadcast	Specifies the broadcast network type.
non-broadcast	Specifies the non-broadcast network type.
point-to-point	Specifies the point-to-point network type.
point-to-multipoint	Specifies the point-to-multipoint network type.
point-to-multipoint non-broadcast	Specifies the point-to-multipoint non-broadcast network type.
instance instance-id	Configures the specific OSPFv3 instance on the interface with the valid id range from 0 to 255.

Defaults Point-to-point network type: PPP, SLIP, frame relay point-to-point sub-interface and X.25 point-to-point sub-interface encapsulation.
 NBMA network type: frame relay(except for the point-to-point sub-interface) and X.25 encapsulation (except for the point-to-point sub-interface)
 Broadcast network type: Ethernet encapsulation.
 The point-to-multipoint network type is not the default type.

Command Mode Interface configuration mode.

Usage Guide You can set the network type of the interface according to the actual link type applied and the topology.

Configuration Examples The following example sets the network type of the interface that participates in the OSPFv3 to point-to-point.

```
ipv6 ospf network point-to-point
```

Related Commands	Command	Description
	ipv6 ospf priority	Sets the interface priority.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description N/A

3.30 ipv6 ospf priority

Use this command to set the interface priority. Use the **no** form of this command to restore the default setting.

ipv6 ospf priority *number-value* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter Description	Parameter	Description
	<i>number-value</i>	The priority of the interface. Its range is from 0 to 255.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface. Its range is from 0 to 255.

Defaults The default priority is 1.

Command Mode Interface configuration mode.

Usage Guide In the broadcast network type, it is necessary to elect the DR/BDR. In electing the DR/BDR, the device of a higher priority is preferred. If several devices are of the same priority, the one with the largest router-ID is preferred.

The device with the priority level of 0 does not participate in the election of DR/BDR.

Configuration Examples The following example disables the interface from being elected as the DR/BDR.

```
ipv6 ospf priority 0
```

Related Commands	Command	Description
	ipv6 ospf network	Sets the network type of an interface.
	router-id	Sets the ID of a router.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.

Platform Description N/A

3.31 ipv6 ospf retransmit-interval

Use this command to set the interval for the interface to retransmit the LSA. Use the **no** form of this command to restore the default setting.

```
ipv6 ospf retransmit-interval seconds [ instance instance-id ]
```

```
no ipv6 ospf retransmit-interval [ instance instance-id ]
```

Parameter Description	Parameter	Description
	<i>seconds</i>	Interval for retransmitting the LSA. Its range is from 1 to 65535 in the unit of seconds.

instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.
------------------------------------	---

Defaults The default is five seconds.

Command

Mode Interface configuration mode.

Usage Guide To ensure the reliability of the routing information transmission, the LSA sent to the neighbor shall be acknowledged by the neighbor. You can use this command to set the interval for the acknowledgement by the neighbor. If no acknowledgement is received within the specified period, the LSA information will be retransmitted.

Configuration The following example sets the interval for retransmitting the LSA to 10 seconds.

Examples

```
ipv6 ospf retransmit-interval 10
```

**Related
Commands**

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform N/A

Description

3.32 ipv6 ospf subvlan

Use this command to enable OSPFv3 on super VLANs. Use the **no** form of this command to restore the default setting.

ipv6 ospf subvlan [all | vid]

no ipv6 ospf subvlan

**Parameter
Description**

Parameter	Description
all	Indicates that packets are allowed to be sent to all sub VLANs.
vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults The default setting takes effect only on super VLANs with OSPFv3 disabled.

Command

Interface configuration mode.

Mode

Usage Guide In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the

device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the OSPF function does not need to be enabled on a super VLAN. Therefore, the OSPF function is disabled by default. However, in some scenarios, the OSPF function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration The following example sends the OSPF multicast packets to sub VLAN 1024 of super VLAN 300.

Examples

```
Ruijie(config)# interface vlan 300
Ruijie(config-if-VLAN 300)# ipv6 ospf subvlan 1024
```

3.33 ipv6 ospf transmit-delay

Use this command to set the delay on the interface in sending the LSA. Use the **no** form of this command to restore the default setting.

ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]

no ipv6 ospf transmit-delay [**instance** *instance-id*]

Parameter Description

Parameter	Description
<i>seconds</i>	The delay in sending LSA. Its range is from 1 to 65535 in the unit of seconds.
instance <i>instance-id</i>	Configures the ID of a specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults The default is one.

Command Mode Interface configuration mode.

Usage Guide Use this command to set the delay on the interface in transmitting the LSA.

Configuration Examples The following example sets the delay on the interface in transmitting the LSA.

```
ipv6 ospf transmit-delay 2
```

Related Commands

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description N/A

3.34 ipv6 router ospf

Use this command to start the OSPFv3 routing process. Use the **no** form of this command to restore the default setting.

ipv6 router ospf

ipv6 router ospf *process-id* [**vrf** *vrf-name*]

no ipv6 router ospf *process-id*

Parameter Description

Parameter	Description
<i>process-id</i>	OSPFv3 process ID number. Without the process number configured, it indicates that process 1 is started.
<i>vrf-name</i>	Specifies the VRF that OSPFv3 process belongs to.

Defaults No OSPFv3 routing process is started.

Command

Mode Global configuration mode.

Usage Guide After the OSPFv3 process is started, the routing process configuration mode is entered. At present, our products support up to 32 OSPFv3 processes.

Configuration The following example starts OSPFv3 process in the specified VRF VPN1.

Examples Ruijie(config)# `ipv6 router ospf 1 vrf vpn_1`

Related Commands

Command	Description
ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform N/A

Description

3.35 ipv6 router ospf max-concurrent-dd

Use this command to set the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes. Use the **no** form of this command to restore the default setting.

ipv6 router ospf max-concurrent-dd *number*

no ipv6 router ospf max-concurrent-dd

Parameter

Parameter	Description
-----------	-------------

Description	
	<i>number</i>

Maximum concurrent interacting neighbors, in the range from 1 to 65535.

Defaults The default is 5.

Command Mode Global configuration mode

Usage Guide When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes can be restricted.

Configuration Examples The following example sets the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
Ruijie#conf terminal
Ruijie(config)#ipv6 router ospf max-concurrent-dd 4
```

Related Commands	Command	Description
	max-concurrent-dd	Sets the maximum concurrent interacting neighbors in the OSPFv3 processes

Platform Description N/A

3.36 log-adj-changes

Use this command to enable the logging of adjacency changes. Use the **no** form of this command to restore the default setting.

log-adj-changes
no log-adj-changes

Parameter Description	Parameter	Description
	detail	Displays details of adjacency changes

Defaults By default, the adjacency state log on the entry of or exit from the FULL state is output.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration The following example turns on the log of adjacency state change.

```
Ruijie(config)# router ospf 1
Ruijie(config)# log-adj-changes detail
```

**Related
Commands**

Command	Description
show ipv6 ospf	Displays the OSPF global configuration information

Platform N/A

Description

3.37 max-concurrent-dd

Use this command to set the maximum number of DD packets that can be processed concurrently in the OSPFv3 routing process. Use the **no** form of this command to restore the default setting.

max-concurrent-dd *number*

no max-concurrent-dd

**Parameter
Description**

Parameter	Description
<i>number</i>	Maximum number of DD packets that can be processed concurrently, in the range from 1 to 65535.

Defaults The default is 5.

Command

Mode Routing process configuration mode.

Usage Guide When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in each OSPFv3 instance can be restricted.

**Configuration
Examples** The following example sets the maximum concurrent interacting neighbors allowed in the current OSPFv3 routing process to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
router ipv6 ospf 1
max-concurrent-dd 4
```

Related Commands	Command	Description
	ipv6 router ospf max-concurrent-dd	Sets the maximum concurrent interacting neighbors allowed in the OSPFv3 processes.

Platform N/A
Description

3.38 passive-interface

Use this command to set the passive interface. Use the **no** form of this command to restore the default setting.

passive-interface { **default** | *interface-type interface-number* }
no passive-interface { **default** | *interface-type interface-number* }

Parameter Description	Parameter	Description
	default	Sets all the interfaces to passive ones.
	<i>interface-type</i> <i>interface-number</i>	Sets the specified interface to a passive one.

Defaults No passive interface is set by default.

Command Mode Routing process configuration mode

Usage Guide After an interface is set to a passive one, it no longer receives or sends the hello message. This command applies to the interfaces participating in the OSPFv3 but not to the virtual links.

Configuration Examples The following example enables only the VLAN1 interface to participate in the OSPFv3 process.

```
passive-interface default
no passive-interface vlan 1
```

Related Commands	Command	Description
	ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
	show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.

Platform N/A
Description

3.39 redistribute

Use this command to start the route redistribution in order to import the routing information of other routing protocols to the OSPFv3 routing process. Use the **no** form of this command to restore the default setting.

```
redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | rip | static } [ { level-1 | level-1-2 | level-2 } | match { internal | external [ 1|2 ] | nssa-external [ 1 | 2 ] } | metric metric-value | metric-type { 1|2 } | route-map route-map-name | tag tag-value ]
no redistribute { bgp | connected | isis [ area-tag ] | ospf process-id | rip | static } [ { level-1 | level-1-2 | level-2 } | match { internal | external [ 1|2 ] | nssa-external [ 1 | 2 ] } | metric | metric-type { 1|2 } | route-map route-map-name | tag tag-value ]
```

Parameter Description

Parameter	Description
bgp	The bgp protocol is redistributed.
connected	The directly connected route is redistributed.
isis [<i>area-tag</i>]	The isis is redistributed. The area-tag specifies a particular isis instance.
ospf <i>process-id</i>	The ospf is redistributed. The process-id specifies a particular ospf instance within the range of 1-65535.
rip	The rip is redistributed.
static	The static route is redistributed.
level-1 level-1-2 level-2	It is used in the IS-IS route redistribution only and redistributes the routes at a specified level. .
match	It is used in the OSPFv3 route redistribution only and filters specific routes for redistribution; internal: inter-area and intra-area routes. external [1 2]: E1, E2 or all external routes. Nssa-external [1 2]: N1, N2 or all external routes of the NSSA area. All sub-type OSPFv3 routes are redistributed by default.
metric <i>metric-value</i>	Specifies the metric for the OSPFv3 external 2 LSA with metric-value. Its range is 0 to 16777214.
metric-type { 1 2 }	Set the metric type for the external route to E-1 or E-2.
route-map <i>map-map-name</i>	Specifies the routing policy for route redistribution. The name of map-tag can be composed of up to 32 characters. No route-map is associated by default.
tag <i>tag-value</i>	Specifies the tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.

Defaults

The function is disabled by default;

Metric-type: 2;

Level-2 routes are redistributed in the ISIS redistribution

OSPFv3 routes of all sub-types are redistributed in the OSPFv3 redistribution
No route-map is associated

Command

Mode Routing process configuration mode

Usage Guide

When a device supports multiple routing protocols, the coordination between these protocols becomes an important task. The device can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

The parameters *level-1*, *level-2* or *level-1-2* can be configured in the redistribution of the ISIS routes to indicate the level of the routes in the redistribution. By default, the level-2 ISIS routes are redistributed

When redistributing OSPFv3 routes, you can configure *match* to redistribute the routes of the corresponding sub-type among the redistributed OSPFv3 routes. All types of OSPFv3 routes are redistributed by default.

The *match* parameter of route-map is specific to the source of routes. The parameters *tag*, *metric* and *metric-type* of the set rule of route-map take precedence over the ones configured for the redistribute command.



The metric value of the route-map associated should be in the range of 0 to 16777214. If the metric value is not in this range, the route cannot be introduced.

The rules for the **no** form of the **redistribute** command are as follows:

If some parameters are specified in the no command, restore their default settings;

If no parameters are specified in the **no** command, delete the whole command.

For example, if the configuration is made below:

Now modify the configuration with the command `no redistribute isis 112 level-2`

According to the above rules, the command only restores level-2 to default and level-2 is default per se, so after the above no command is executed, the configuration remains as `redistribute isis 112 level-2`

To delete the whole command, use the command below

Configuration

The following example redistributes the direct route and associates route-map test :

Examples

```
ipv6 router ospf 1
redistribute connect metric 10 route-map test
```

The associated route-map is configured as follows:

```
route-map test permit 10
match metric 20
set metric 30
```

The effect of the above configuration is to set the metric value which is 20 of the redistributed routes to 30, and that of other routes to 10

Related Commands

Command	Description
<code>default-information originate</code>	Sets the default route to be redistributed.

default-metric	Sets the default metric for the route to be redistributed.
summary-prefix	Sets the converged address range of the external route.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

Platform N/A

Description

3.40 router-id

Use this command to set the router ID (device ID). Use the **no** form of this command to restore the default setting.

router-id *router-id*

no router-id

Parameter Description	Parameter	Description
	<i>router-id</i>	ID of the device in the IPv4 address format.

Defaults The OSPFv3 routing process, the largest IPv4 address of all loopback interfaces is elected as the router ID; If there is no loopback interface with an IPv4 address, the OSPFv3 process will elect the largest IPv4 of all other interfaces as the router ID

Command Mode Routing process configuration mode

Usage Guide Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the format of IPv4 address.

Any IPv4 address can be set as the router ID, but the router ID of every routers in the AS must be unique. If multiple OSPFv3 processes are running on the same device, the router ID of every process must be unique. Note that the change of the router ID results in considerable processing work in the protocol. Therefore, it is not recommended to change any router ID without proper reason. A prompt will be given to ask whether you are sure to modify the router ID. It is recommended that you specify a router ID once an OSPFv3 process starts before configuring other parameters for the process

Configuration Examples The following example sets the ID of the device that participates in the OSPFv3 process to 1.1.1.1.

```
router-id 1.1.1.1
```

Related Commands	Command	Description
------------------	---------	-------------

ipv6 ospf priority	Sets the interface priority.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform N/A

Description

3.41 show ipv6 ospf

Use this command to display the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter Description	Parameter	Description
	<i>process- id</i>	OSPF process ID number.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the information about the OSPFv3 process.

Examples

```
Ruijie# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
Enable two-way-maintain
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Initial LSA throttle delay 0 msec
Minimum hold time for LSA throttle 5000 msec
Maximum wait time for LSA throttle 5000 msec
Lsa Transmit Pacing timer 40 msec, 1 LS-Upd
LSA interval 5 secs, Minimum LSA arrival 1000 msec
Pacing lsa-group: 30 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 11
Number of LSA received 4
Log Neighbor Adjacency Changes : Enabled
Number of areas in this router is 2
Area BACKBONE(0)
```

```

Number of interfaces in this area is 1(1)
SPF algorithm executed 4 times
Number of LSA 3. Checksum Sum 0x1DDF1
Number of Unknown LSA 0
  Area 0.0.0.1 (NSSA)
    Number of interfaces in this area is 1(1)
    SPF algorithm executed 5 times
    Number of LSA 7. Checksum Sum 0x445FE
    Number of Unknown LSA 0

```

**Related
Commands**

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
default-information originate	Sets the default route to be redistributed.
default-metric	Sets the default metric for the route to be redistributed.
<i>router-id</i>	Sets the OSPFv3 routing process ID
timers spf	Sets the delay and the minimum and maximum intervals for the OSPFv3 to perform SPF calculation after receiving the topology change information.

Platform N/A
Description

3.42 show ipv6 ospf database

Use this command to display the database information of the OSPFv3 process

show ipv6 ospf [*process-id*] **database** [*lsa-type* [**adv-router** *router-id*]]

**Parameter
Description**

Parameter	Description
<i>process-id</i>	OSPF process ID number
<i>lsa-type</i>	The LSA types are as follows: NSSA-external-LSA, AS-external-LSAs, Link-LSAs, Inter-Area-Prefix-LSAs, Inter-Area-Router-LSAs, Intra-Area-Prefix-LSAs, Network-LSAs, Router-LSAs If this parameter is not specified, all LSA information will be displayed.
adv-router <i>router-id</i>	Displays the LSA information generated by the specified router.

Defaults N/A

Command Privileged EXEC mode.

Mode**Usage Guide** N/A**Configuration** The following example displays the information about the OSPFv3 process database.**Examples**

```

Ruijie# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface FastEthernet 1/0)
Link State ID  ADV Router      Age  Seq#      CkSum  Prefix
0.0.0.2        1.1.1.1      197  0x80000001 0x7cd8  0
0.0.0.5        2.2.2.2      206  0x80000001 0x8c86  0

      Link-LSA (Interface Loopback 1)
Link State ID  ADV Router      Age  Seq#      CkSum  Prefix
0.0.64.1      1.1.1.1        82  0x80000001 0xb760  0

      Router-LSA (Area 0.0.0.0)
Link State ID  ADV Router      Age  Seq#      CkSum  Link
0.0.0.0        1.1.1.1        17  0x80000006 0x62a1  1
0.0.0.0        2.2.2.2        156 0x80000003 0x8653  1

      Network-LSA (Area 0.0.0.0)
Link State ID  ADV Router      Age  Seq#      CkSum
0.0.0.5        2.2.2.2        157 0x80000001 0xf8f6

      Router-LSA (Area 0.0.0.1)
Link State ID  ADV Router      Age  Seq#      CkSum  Link
0.0.0.0        1.1.1.1        17  0x80000002 0x0529  0

      Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID  ADV Router      Age  Seq#      CkSum
0.0.0.1        1.1.1.1        77  0x80000002 0x83b4

AS-external-LSA
Link State ID  ADV Router      Age  Seq#      CkSum
0.0.0.1        1.1.1.1        1  0x80000001 0x6035  E2

```

**Related
Commands**

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform N/A**Description**

3.43 show ipv6 ospf interface

Use this command to display the OSPFv3 interface information.

show ipv6 ospf [*process-id*] **interface** [*interface-type interface-number* | **brief**]**Parameter**

Parameter	Description
-----------	-------------

Description	
<i>interface-type</i> <i>interface-number</i>	Specifies the interface type and interface number.
<i>process-id</i>	OSPFv3 process ID
brief	Displays the interface summary.

Defaults N/A

Command Privileged EXEC mode.

Mode

Usage Guide N/A

Configuration The following example displays the information about the OSPFv3 interface.

Examples

```
Ruijie# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

If the BFD has been enabled for the neighbor on the interface, the content of "BFD enabled" is also displayed. For example:

```
Ruijie# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1, BFD enabled
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
```

```
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

Related Commands

Command	Description
<code>ipv6 router ospf</code>	Starts the OSPFv3 routing process.
<code>ipv6 ospf area</code>	Enables the interface to participate in the OSPFv3 process.

Platform N/A

Description

3.44 show ipv6 ospf neighbor

Use this command to display the neighbor information of the OSPFv3 process.

```
show ipv6 ospf [ process-id ] neighbor [ interface-type interface-number [ detail ] ] neighbor-id
[detail ]
```

Parameter Description

Parameter	Description
<i>process-id</i>	OSPFv3 process ID number
detail	Displays details about the neighbor.
<i>interface-type</i> <i>interface-number</i>	Interface type and interface number
<i>neighbor-id</i>	Neighbor's router ID

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide N/A

Configuration The following command displays the brief information about the OSPFv3 neighbor.

Examples

```
Ruijie# show ipv6 ospf neighbor
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:
Neighbor ID  Pri  State      Dead Time   Interface          Instance ID
2.2.2.2      1    Full/DR   00:00:33   FastEthernet 1/0  0
```

```
Ruijie# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
In the area 0.0.0.0 via interface FastEthernet 1/0
Neighbor priority is 1, State is Full, 6 state changes
DR is 2.2.2.2 BDR is 1.1.1.1
Options is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:36
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
BFD session state up
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.
area virtual-link	Configures the OSPFv3 virtual link.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform N/A

Description

3.45 show ipv6 ospf restart

Use this command to display the OSPFv3 graceful restart configuration.

show ipv6 ospf [*process-id*] restart

Parameter Description

Parameter	Description
<i>process-id</i>	OSPFv3 process ID number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the restarter status.

```
Ruijie# show ipv6 ospf restart
Routing Process is ospf 1
Graceful-restart enabled
Restart grace period 120 secs
```

```
Current Restart status is plannedRestart
Current Restart remaining time 50 secs
Graceful-restart helper support enabled
```

The following example displays the helper status.

```
Ruijie# show ipv6 ospf restart
Routing Process is ospf 1
Neighbor 10.1.1.2, interface addr 10.1.1.2
In the area 0.0.0.0 via interface GigabitEthernet 6/0/0
Graceful-restart helper enabled
Current helper status is helping
Current helper remaining time 50 secs
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform N/A
Description

3.46 show ipv6 ospf route

Use this command to display the OSPFv3 route information.

show ipv6 ospf [*process-id*] route [*count*]

Parameter Description

Parameter	Description
<i>process-id</i>	OSPFv3 process ID number.
count	Total number of OSPFv3 routes

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the information about OSPFv3 routes.

Examples

```
Ruijie# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
Destination
Metric  Next-hop
```

```
E2 2001:DB8:1::/64 1/20 via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O 2001:DB8:2::/64 11 via fe80::c800:eff:fe84:1c, FastEthernet 1/0,
Area 0.0.0.0
```

**Related
Commands**

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform N/A**Description**

3.47 show ipv6 ospf summary-prefix

Use this command to display the external route convergence information of OSPFv3

show ipv6 ospf [*process-id*] summary-prefix

**Parameter
Description**

Parameter	Description
<i>process-id</i>	OSPFv3 process ID number

Defaults N/A**Command
Mode** Privileged EXEC mode.**Usage Guide** N/A**Configuration** The following example displays the external route convergence information of OSPFv3.**Examples**

```
Ruijie# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:db8::/64, Metric 16777215, Type0, Tag0, Match count0, advertise
```

**Related
Commands**

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
summary-prefix	Configures the converge route outside the OSPFv3 routing domain.

Platform N/A**Description**

3.48 show ipv6 ospf topology

Use this command to display the topology information about each area of OSPFv3.

show ipv6 ospf [*process-id*] **topology** [**area** *area-id*]

Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number
	<i>area-id</i>	Area ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following command displays the topology information about each area of OSPFv3.

Examples

```
Ruijie# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID      Bits  Metric  Next-Hop
Interface
1.1.1.1        EB   --
2.2.2.2        E    1       2.2.2.2
FastEthernet 1/0

OSPFv3 paths to Area (0.0.0.1) routers
Router ID      Bits  Metric  Next-Hop
Interface
1.1.1.1        B    --
```

Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	area range	Configures the address range of the OSPF area.

Platform Description N/A

3.49 show ipv6 ospf virtual-links

Use this command to display the virtual link information of the OSPFv3 process

show ipv6 ospf [*process-id*] **virtual-links**

Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following command displays the information about the OSPFv3 virtual link.

Examples

```
Ruijie# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 2.2.2.2 is down
  Transit area 0.0.0.1 via interface FastEthernet 1/0, instance ID 0
  Local address *
  Remote address 3333::1/128
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in inactive
  Adjacency state Down
```

Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	area virtual-link	Configures the OSPFv3 virtual link.
	show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.

Platform Description N/A

3.50 summary-prefix

Use this command to configure the converged route outside the OSPFv3 routing domain in the routing process configuration mode. Use the **no** form of this command to restore the default setting.

summary-prefix *ipv6-prefix/prefix-length* [**not-advertise** | **tag** < 0-4294967295 >]

no summary-prefix *ipv6-prefix/prefix-length* [**not-advertise** | **tag** < 0-4294967295 >]

Parameter Description	Parameter	Description
	<i>ipv6-prefix/prefix-length</i>	Address range of the converged route
	not-advertise	Does not advertise the converged route to neighbors. Absence of this parameter means to advertise.
	tag <0-4294967295>	Tag value redistributed to the OSPFv3 inner route, in the range from 0 to 4294967295.

Defaults No converged route is configured by default.

Command Mode Routing process configuration mode.

Usage Guide When routes are redistributed by another routing process into the OSPFv3 routing process, every route is advertised to the OSPFv3-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous system border device can advertise only one converged route, thus reducing the scale of routing table greatly.

It is different from the **area range** command. The area range involves the convergence of routes between OSPFv3 areas, while the **summary-prefix** involves the convergence of external routes of the OSPFv3 routing domain.

Configuring the **summary-prefix** command on the ASBR can perform convergence for only redistributed routes; while configuring this command on the NSSA ABR translator can perform convergence for the redistributed routes and the Type-5 routes translated from Type-7.

Configuration Examples The following example configures the external route within the 2001:DB8::/64 to the converged route 2001:DB8::/64 to advertise it.

```
summary-prefix 2001 :DB8 : : /64
```

Related Commands	Command	Description
	area-range	Configures route convergence between the OSPFv3 areas.
	redistribute	Redistributes the routes in other routing process.

Platform Description N/A

3.51 timers lsa arrival

Use this command to configure a delay for receiving repeated LSAs. Use the **no** form of this command to restore the default setting.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>arrival-time</i></td> <td>Specifies the delay for receiving repeated LSAs. The range is from 0 to 600000 in the unit of milliseconds.</td> </tr> </tbody> </table>	Parameter	Description	<i>arrival-time</i>	Specifies the delay for receiving repeated LSAs. The range is from 0 to 600000 in the unit of milliseconds.
Parameter	Description				
<i>arrival-time</i>	Specifies the delay for receiving repeated LSAs. The range is from 0 to 600000 in the unit of milliseconds.				
Defaults	The default is 1000.				
Command Mode	Routing process configuration mode				
Usage Guide	Configure the device not to process repeated LSAs received within the specific delay.				
Configuration Examples	The following example sets the delay for receiving repeated LSAs to 2 seconds. <pre>Ruijie(config)# ipv6 router ospf 1 Ruijie(config-router)# timers lsa arrival 2000</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show ipv6 ospf</td> <td>Displays OSPFv3 process information, including identifiers of routing devices.</td> </tr> </tbody> </table>	Command	Description	show ipv6 ospf	Displays OSPFv3 process information, including identifiers of routing devices.
Command	Description				
show ipv6 ospf	Displays OSPFv3 process information, including identifiers of routing devices.				
Platform Description	N/A				

3.52 timers pacing lsa-group

Use this command to set an LSA group pace interval. Use the **no** form of this command to restore the default setting.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter Description	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>seconds</td> <td>Specifies the LSA group pace interval. The range is from 10 to 1800 in the unit of seconds. The default value is 30.</td> </tr> </tbody> </table>	Parameter	Description	seconds	Specifies the LSA group pace interval. The range is from 10 to 1800 in the unit of seconds. The default value is 30.
Parameter	Description				
seconds	Specifies the LSA group pace interval. The range is from 10 to 1800 in the unit of seconds. The default value is 30.				
Defaults	The default is 30.				
Command Mode	Routing process configuration mode				
Usage Guide	Each LSA has its own lifetime, that is, LSA aging time. An LSA existing for 1800s will be refreshed so that the living time of the LSA will not exceed its aging time. This ensures that normal LSAs are not				

cleared due to timeout of aging time. If update and aging operations of each LSA are separately computed, a large number of CPU resources will be consumed.

To effectively utilize CPU resources, configure the device to group LSAs for uniform refreshment. The time for refreshing a group of LSAs is called an LSA group pace interval. Grouping refreshment is to put the LSAs to be refreshed within an LSA group pace interval into a group and refresh them uniformly.

When the number of LSAs is fixed, a longer LSA group pace interval will allow the CPU to process more LSAs when the timer expires for one time. To keep the stability of the CPU, you are recommended not to set an over long LSA group pace interval. This prevents the CPU from processing excessive LSAs when the timer expires each time. If the CPU processes a large number of LSAs each time, it is recommended to shorten the LSA group pace interval. For example, if the database has 10000 LSAs, you need to reduce the LSA group pace interval. If it has only 40 to 100 LSAs, you can adjust the group pace interval to 10 through 20 minutes.

Configuration The following example sets the LSA group pace interval to 120 seconds.

Examples

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)#timers pacing lsa-group 120
```

**Related
Commands**

Command	Description
show ipv6 ospf	Displays OSPFv3 configuration information.

Platform N/A
Description

3.53 timers pacing lsa-transmit

Use this command to set an interval for sending LSA groups. Use the **no** form of this command to restore the default setting.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

**Parameter
Description**

Parameter	Description
<i>transmit-time</i>	Specifies the interval for sending LSA groups. The range is from 10 to 1000 in the unit of milliseconds.
<i>transmit-count</i>	Specifies the number of LS-UPD packets in an LSA group. The range is from 1 to 200.

Defaults The default transmit-time is 40 and the transmit-count is 1.

**Command
Mode** Routing process configuration mode

Usage Guide There are usually a lot of LSAs on a network; therefore, the load of the device is very high. Setting proper **transmit-time** and **transmit-count** values can restrict flooding of LS-UPD packets on the network.

When the CPU load is not high and network bandwidth usage is not large, you can reduce the **transmit-time** value and increase the **transmit-count** value to accelerate route convergence.

Configuration Examples The following example sets the interval for sending LS-UPDs to 50 milliseconds and the specified 20 packets to be sent each time.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information.

Platform N/A
Description

3.54 timers spf

Use this command to set the delay and interval for the OSPFv3 to calculate SPF after receiving the topology change. Use the **no** format of this command to restore the default setting.

timers spf delay holdtime
no timers spf

Parameter Description

Parameter	Description
<i>spf-delay</i>	Defines the waiting time for the SPF calculation, which ranges from 0 to 214748364 seconds. After receiving the topology change information, the OSPF routing process has to waiting for a given period before making the SPF calculation.
<i>spf-holdtime</i>	Defines the interval between two SPF calculations, which ranges from 0 to 214748364 seconds. If the interval has not passed even if the waiting time has elapsed, no SPF calculation can be made yet.

Defaults There are two default situations: 1. The versions earlier than RGOS 10.4 do not support the command **timers throttle spf**. The system default is **timers spf 5 10**. 2. The RGOS 10.4 and the later versions do support the command **timers throttle spf**, where **timer spf** takes no effect by default. The delay for SPF calculation is subject to the default setting of the command **timers throttle spf**. Refer to the description of the command.

Command Mode Routing process configuration mode

Usage Guide The smaller the *spf-delay* and *spf-holdtime*, the shorter time the OSPF takes to adapt to the topology change, but the more CPU time will be used of the router.

 The **timer spf** configuration and the **timers throttle spf** configuration will overwrite each other.

Configuration Examples The following example sets the delay and holdtime of the OSPFv3 to 3 seconds and 9 seconds respectively.

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# timers spf 3 9
```

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the function of the OSPFv3.
show ipv6 ospf	Displays the OSPFv3 routing process information.
timers throttle spf	Configures the exponential backoff delay of the SPF calculation

Platform N/A

Description

3.55 timers throttle lsa all

Use this command to configure an exponential backoff algorithm for generating LSAs. Use the **no** form of this command to restore the default setting.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description


Parameter	Description
<i>delay-time</i>	Specifies a shortest LSA generation delay, in milliseconds (the first batch of LSAs is usually generated immediately). The range is from 0 to 600000 in the unit of milliseconds.
<i>hold-time</i>	Specifies a shortest interval between the first two times of LSA refreshment, in milliseconds. The range is from 1 to 600000 in the unit of milliseconds
<i>max-wait-time</i>	Specifies a longest interval for consecutive two times of LSA refreshment, in milliseconds. The value is used to determine whether LSAs are refreshed consecutively. The range is from 1 to 600000 in the unit of milliseconds.

Defaults The default *delay-time* is 0, *hold-time* is 5000 and *max-wait-time* is 5000.

Command Routing process configuration mode

Mode

Usage Guide If high route convergence capability is needed when links are changed, set a small *delay-time* value. To reduce CPU consumption, you can properly increase the values of the parameters.

 The *hold-time* value cannot be smaller than the *delay-time* value and must be smaller than or equal to the *max-wait-time* value.

Configuration Examples The following example sets *delay-time* to 10 milliseconds, *hold-time* to one second, and *max-wait-time* to five seconds.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
<code>show ipv6 ospf</code>	Displays OSPFv3 process information.

Platform N/A

Description

3.56 timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default setting.

timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
<i>ia-delay</i>	Sets the delay time of the inter-area route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the <i>ia-delay</i> time runs out.
ase	Calculates the external routes.
<i>ase-delay</i>	Sets the delay time of the external route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the <i>ase-delay</i> time runs out.

Defaults The default *ia-delay* is 0 and *ase-delay* is 0.

Command Routing process configuration mode

Mode

Usage Guide The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration The following example sets the delay time of the inter-area route calculation to one second.

Examples

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.57 timers throttle spf

Use this command to configure, the delay for SPF calculation as well as the minimum and maximum intervals between two SPF calculations after receiving the topology change information for OSPFv3 in the routing process configuration mode. Use the **no** form of this command to restore the default setting.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
<i>spf-delay</i>	Specifies an SPF calculation delay after the topology change information is received. The range is from 1 to 600000 in the unit of milliseconds.
<i>spf-holdtime</i>	Specifies a shortest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.
<i>spf-max-waittime</i>	Specifies a longest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.

Defaults The default *spf-delay* is 1000. *spf-holdtime* is 5000 and *spf-max-waittime* is 10000.

Command

Mode Routing process configuration mode.

Usage Guide *Spf-delay* refers to the delay from the topology change to the SPF calculation. *Spf-holdtime* refers to the minimum interval between the first and the second SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval till it reaches to *spf-max-waittime*. If

the interval between two SPF calculations has exceeded the required minimum value, the interval of SPF calculation will re-start from *spf-holdtime*.

Smaller *spf-delay* and *spf-holdtime* value can make the topology convergence faster. Greater *spf-max-waittime* value can reduce the SPF calculations. Those configuration are flexible according to the actual stability of the network topology.

Compared with the timers spf command, this command is more flexible. It not only speeds up the SPF convergence calculation, but also reduces the system resources consumption of SPF calculation as the topology changes continuously. Therefore, the timers throttle spf command is recommended.

- i The spf-holdtime cannot be smaller than spf-delay, or the spf-holdtime will be set to be equal to spf-delay;
- i The spf-max-waittime cannot be smaller than spf-holdtime, or the spf-max-waittime will be set to be equal to spf-holdtime automatically;
- i The configuration of the timers spf command and of the timers throttle spf command are overwritten each other.
- i With neither timers spf command nor timers throttle spf command configured, the default value refers to the default of the timers throttle spf command

Configuration Examples The following example configures the delay and holdtime and the maximum time interval of the OSPFv3 as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the time for SPF calculation is: five milliseconds, one second, three seconds, seven seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90 seconds.....

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# timers spf 5 1000 90000
```

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the OSPFv3 function.
show ipv6 ospf	Displays the routing process information of the OSFPv3
timers spf	Configures the SPF calculation delay .

Platform N/A
Description

3.58 two-way-maintain

Use this command to enable two-way OSPFv3 maintenance. Use the **no** form of this command to disable this function.

two-way-maintain
no two-way-maintain

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	N/A	N/A

Defaults Two-way OSPFv3 maintenance is enabled by default.

Command Mode Routing process configuration mode

Usage Guide Sometimes, there are a lot of sent and received packets on a network, occupying large CPU and memory resources. As a result, some packets cannot be processed immediately or are directly lost. If hello packets from a neighbor cannot be processed within the dead interval of neighbors, the connection with the neighbor will be interrupted due to connection timeout. If two-way OSPFv3 maintenance is enabled and a large number of packets exist on the network, besides hello packets, the two-way neighboring relationship between the device and the neighbor can also be maintained by DD, LSU, LSR, and LSAck packets from the neighbor. This prevents the neighboring relationship from failing due to receiving delay or discarding of hello packets.

Configuration The following example disables two-way OSPFv3 maintenance.

Examples

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# no two-way-maintain
```

Related Commands	Command	Description
		show ipv6 ospf

Platform Description N/A

4 IS-IS Commands

4.1 address-family ipv6

Use this command to enter the **address-family ipv6** mode. Use the **no** form of this command to delete all configurations in the **address-family ipv6**.

address-family ipv6 [*unicast*]

no address-family ipv6 [*unicast*]

Parameter Description	Parameter	Description
	<i>unicast</i>	IPv6 unicast address prefix.

Defaults By default, no address-family ipv6 is configured.

Command Mode IS-IS routing process configuration mode

Usage Guide This command is used for the IPv6 special configurations.
To exit to the IS-IS routing process configuration mode, use the **exit-address-family** command.

Configuration

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# address-family ipv6 unicast
```

Related Commands	Command	Description
	exit-address-family	Exits the address-family ipv6 mode.

Platform Description N/A

4.2 adjacency-check

Use this command to detect protocols supported by the adjacency in the Hello packets. Use the **no** form of this command is to cancel this detection.

adjacency-check

no adjacency-check

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults By default, this detection is enabled.

Command Mode IS-IS routing process configuration mode or address-family ipv6 mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# adjacency-check
Ruijie(config-router)# address-family ipv6
Ruijie(config-router-af)# adjacency-check
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.3 area-password

Use this command to set the plain-text authentication password for the Level-1 area. Use the **no** form of this command to cancel the password set.

area-password [0 | 7] *password-string* [**send-only**]
no area-password [**send-only**]

Parameter Description

Parameter	Description
0	Indicates that the key is displayed in plaintext.
7	Indicates that the key is displayed in ciphertext.
<i>password-string</i>	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
send-only	Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticate.

Defaults By default, no authentication password is set.

Command Mode IS-IS routing process configuration mode

Usage Guide Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-1 areas

and include authentication information in these packets before they are sent. All IS-IS devices in an area must be configured with the same password.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no area-password** command. If you run the **no area-password send-only** command, only the **send-only** setting is canceled. If you run the **area-password psw send-only** and **no area-password send-only** commands in sequence, the configuration is changed to **area-password psw**.

Configuration Examples The following example specifies the authentication in the IS-IS area using the plaintext mode with the password being *redgiant* and the password applicable to the packets sent only, but not to the packets received.

```
Ruijie(config)# router isis
Ruijie(config-router)# area-password redgiant send-only
```

Related Commands

Command	Description
domain-password	Sets the Level-2 domain password.
authentication mode	Specifies the IS-IS authentication mode.

Platform Description N/A

4.4 authentication key-chain

Use this command to specify the key-chain used by the IS-IS authentication. Use the **no** form of this command to cancel the key-chain specified.

authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Parameter Description

Parameter	Description
<i>name-of-chain</i>	Key-chain name with the maximum length being 255.
level-1	Specifies the authentication key-chain of the Level-1.
level-2	Specifies the authentication key-chain of the Level-2.

Defaults By default, the authentication key-chain is not specified.

Command Mode IS-IS routing process configuration mode

Usage Guide If the **key chain** command is not used to configure the corresponding key-chain, the authentication will not be performed. In addition, to make the IS-IS key-chain authentication effective, you need to configure the **authentication mode** command at the same time.

This key-chain can apply to the plain-text authentication mode and MD5 encrypted authentication mode. You can use the **authentication mode** command to set the authentication mode.

The length of the password key-string in the key-chain shall not be larger than 80 characters if the plain-text authentication mode is used, otherwise this configuration will fail.

Only one key-chain is used at one time. So, when configuring this command, the said key-chain will be replaced by the new specified one.

If the Level is not specified, the key-chain will apply to both Level-1 and Level-2.

The key-chain specified by this command works on the LSP, CSNP and PSNP packets. The IS-IS will send or receive the password that belongs to this key-chain.

There may contain multiple passwords in the key-chain. When sending the packets, use the password with small number first. While receiving the packets, the packet will be received as long as the password of this packet received corresponds to any password in the key-chain.

Configuration The following example specifies the authentication in the IS-IS area using the key-chain named *kc*:

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication key-chain kc level-1
```

**Related
Commands**

Command	Description
authentication mode	Specifies the IS-IS authentication mode.
authentication send-only	Specifies the IS-IS authentication applicable to the sent packets only, but not to packets received.
key-chain	Configures the key-chain.

Platform N/A

Description

4.5 authentication mode

Use this command to specify the mode of IS-IS authentication. Use the **no** form of this command to cancel the specified IS-IS authentication mode.

authentication mode { **md5** | **text** } [**level-1** | **level-2**]

no authentication mode { **md5** | **text** } [**level-1** | **level-2**]

**Parameter
Description**

Parameter	Description
md5	Specifies the MD5 authentication mode to use.
text	Specifies the plain-text authentication mode to use.
level-1	Specifies the authentication mode taking effect on the Level-1.
level-2	Specifies the authentication mode taking effect on the Level-2.

Defaults By default, the authentication mode is not specified.

Command IS-IS routing process configuration mode
Mode

Usage Guide To make the key-chain configured by the **authentication key-chain** command effective, you must use the **authentication mode** command to specify the authentication mode.

If no Level is specified, the authentication mode specified is applicable to both Level-1 and Level-2.

When configuring the **authentication mode** command, if the **area-password** or **domain-password** command has been executed to configure the plaintext authentication before, the said commands will be overwritten by the new command.

If the **authentication mode** command has been configured, the **area-password** or **domain-password** will not be configured successfully, you need to delete the **authentication mode** command first.

Configuration The following example specifies authentication in the IS-IS area to be the MD5 authentication mode.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication mode md5 level-1
```

Related Commands

Command	Description
area-password	Sets the area plaintext authentication password.
authentication key-chain	Specifies the key-chain used by the IS-IS authentication.
authentication send-only	Specifies the IS-IS authentication applicable to the packets sent only, but not to the packets received.
domain-password	Sets the domain plaintext authentication password.

Platform N/A
Description

4.6 authentication send-only

Use this command to specify the IS-IS authentication only applicable to the packets sent, but not to the packets received. Use the **no** form of this command to perform the authentication on the packets received.

authentication send-only [level-1 | level-2]

no authentication send-only [level-1 | level-2]

Parameter Description

Parameter	Description
level-1	Specifies setting send-only on the Level-1.
level-2	Specifies setting send-only on the Level-2.

- Defaults** By default, this command is not configured. If the IS-IS authentication is configured, the authentication will be performed on the packets both sent and received.
- Command** IS-IS routing process configuration mode
- Mode**
- Usage Guide** With this command configured, the IS-IS will set the authentication password in the packets sent, however, the authentication will not be performed on the packets received. It can apply to the following two occasions: 1. before deploying the IS-IS authentication for all devices in the network. 2. before changing the authentication password or authentication mode. Before the above two tasks start, you need to configure the **authentication send-only** command first to make each device perform no authentication on the packets received, so as to avoid the network oscillation caused during the subsequent authentication password deployment. After the deployment of the entire network authentication finished, execute the **no isis authentication send-only** command to cancel the **send-only** authentication mode.
- This command can apply to the plain-text authentication mode and MD5 authentication mode. You can use the **authentication mode** command to set the authentication mode.
- If the Level is not specified, the authentication mode specified is applicable to both Level-1 and Level-2.

Configuration The following example specifies the authentication in the IS-IS area to be the **send-only** mode.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication send-only level-1
```

Related Commands	Command	Description
	authentication key-chain	Specifies the IS-IS authentication key-chain.
	authentication mode	Specifies the mode of IS-IS authentication.
	key-chain	Configures the key-chain.

Platform N/A

Description

4.7 bfd all-interfaces

Use this command to configure all interfaces running the IS-IS protocol to conduct BFD link detection.

bfd all-interfaces [anti-congestion]

Use the **no** form of this command to configure all interfaces running the IS-IS protocol to not conduct BFD link detection.

no bfd all-interfaces [anti-congestion]

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	anti-congestion	IS-IS BFD anti-flapping option

Defaults The IS-IS support for BFD is disabled on all interfaces by default.

Command Mode IS-IS routing process configuration mode

Default Level 14

Usage Guide There are two methods for enabling or disabling the IS-IS support for BFD on interfaces.

Method 1: In IS-IS routing process configuration mode, run the [**no**] **bfd all-interfaces [anti-congestion]** command to enable or disable the IS-IS support for BFD on all interfaces running the IS-IS protocol.


Method 2: In interface configuration mode, run the **isis bfd [disable | anti-congestion]** command to enable or disable the IS-IS support for BFD on a specified interface.

In normal cases, the BFD function enables to send detection packets to detect the link status at an interval of several milliseconds. When a link exception such as link interruption occurs, the BFD function enables to rapidly detect the link exception, and notify a device running the IS-IS protocol to delete neighbors and delete neighbor availability information from LSP packets. The device running the IS-IS protocol performs route re-calculation and generates a new route, to bypass the failure link, thereby implementing fast convergence. With the introduction of some new technologies such as the Multi-Service Transport Platform (MSTP), link congestion easily occurs in peak hours. When congestion occurs, the BFD function allows to rapidly detect a link exception, notify a device running the IS-IS protocol to delete a neighbor and delete neighbor availability information from LSP packets, and perform link switching to bypass the congested link. The interval for an IS-IS neighbor to send a Hello detection packet is 10 seconds and the timeout time is 30 seconds. When an exception is detected via the BFD function, IS-IS Hello packets can be normally received, an IS-IS neighbor relationship can be rapidly established, and the route is restored to pass the congested link. Then, BFD is performed again. If there is still a link exception, link switching is performed again, and the process repeats. The route switches between the congested link and other links and flapping occurs.

The anti-flapping function can be enabled to prevent route flapping in the case of link congestion. After the anti-flapping function is enabled, if a link is congested, the IS-IS neighbor status keeps alive but the neighbor availability information in LSP packets is deleted, and the route switches to a non-congested link. After the link is restored, that is, congestion is removed, the neighbor availability information is restored in LSP packets, and the route switches back to the originally congested link, thereby preventing route flapping.

When IS-IS anti-flapping is enabled, the BFD anti-flapping command (**bfd up-dampening**) must be configured on an interface. The two commands must be configured simultaneously. If only one of them is configured, the anti-flapping function does not take effect or a network exception is incurred.

For details about how to enable the BFD anti-flapping function on an interface, see the configuration example of the ISIS BFD command.

-  Before the IS-IS support for BFD is configured, a BFD session must be configured on an interface.
-  When the BFD anti-flapping command is configured on an interface, if the IS-IS support for BFD is

already configured on the interface, the anti-flapping function must be enabled for a device running the IS-IS protocol.

- When the IS-IS anti-flapping option is configured, the BFD anti-flapping command must be configured on an interface.

Configuration The following example configures all interfaces running the IS-IS protocol to conduct BFD.

Examples

```
Ruijie(config)# router isis 123
Ruijie(config-router)# bfd all-interface
```

4.8 clear clns neighbors

Use this command to clear all IS-IS neighbor relation tables.

clear clns neighbors

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used in the condition of needing to refresh the IS-IS neighbor relation table immediately.

Configuration The following example clears all IS-IS neighbor relation tables.

Examples

```
Ruijie# clear clns neighbors
```

Related Commands	Command	Description
	clear isis	Clears all IS-IS data structure.

Platform Description N/A

4.9 clear isis *

Use this command to clear the data structure of all IS-ISs.

clear isis *

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used in the condition of needing to refresh the LSP immediately. For example, after executing the **area-password** and **domain-password** commands, the previous LSPs still exist in this router, you can use this command to clear these LSPs.

Configuration Examples Ruijie# **clear isis ***

Related Commands	Command	Description
		clear clns neighbors

Platform Description N/A

4.10 clear isis counter

Use this command to clear various statistics of IS-IS.

clear isis [tag] counter

Parameter Description	Parameter	Description
		<i>tag</i>

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears various statistics of IS-IS.

Ruijie# **clear isis counter**

Related Commands	Command	Description
---------------------	---------	-------------

clear isis *	Clears the data structure of all IS-ISs.
---------------------	--

Platform N/A

Description

4.11 default-information originate

Use this command to generate a default routing information and advertise it by LSP. Use the **no** form of this command to delete the default routing information from LSP.

default-information originate [**route-map** *map-name*]

no default-information originate [**route-map** *map-name*]

Parameter	Parameter	Description
Description	<i>map-name</i>	(Optional) Associated route-map's name, with the maximum length being 32. By default, the route-map is not associated.

Defaults By default, there is no default route.

Command IS-IS routing process configuration mode or address-family ipv6 mode.

Mode

Usage Guide The default route is not generated in the Level-2 domain. Use this command to allow the default route to enter the Level-2 domain.

Configuration The following example generates a default routing information and advertises it by LSP

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# default-information originate
Ruijie(config-router)# address-family ipv6
Ruijie(config-router-af)# default-information originate
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.12 distance

Use this command to set the management distance of the IS-IS routes. Use the **no** form of this command to restore the default settings.

distance *my-cost*

no distance**Parameter
Description**

Parameter	Description
<i>my-cost</i>	Distance value in the range of 1 to 255.

Defaults By default, the distance is 115.

Command Mode IS-IS routing process configuration mode or IS-IS address-family ipv6 configuration mode

Usage Guide Use this command to configure the management distance of the IS-IS routes. The shorter the management distance, the more reliable the routing information is.

Configuration The following example sets the management distance of the IS-IS routes.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# distance 100
```

**Related
Commands**

Command	Description
isis metric	Sets the metric value of the interface.

Platform N/A
Description

4.13 domain-password

Use this command to set the plain-text authentication password of Level-2 domain. Use the **no** form of this command to cancel the password configured.

domain-password [0 | 7] *password-string* [**send-only**]

no domain-password [**send-only**]

**Parameter
Description**

Parameter	Description
0	Indicates that the key is displayed in plaintext.
7	Indicates that the key is displayed in ciphertext.
<i>password-string</i>	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
send-only	Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticated.

Defaults By default, no authentication password is set.

Command IS-IS routing process configuration mode
Mode

Usage Guide Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-2 domains and include authentication information in these packets before they are sent. All IS-IS devices in a Level-2 domain must be configured with the same password.

This command does not take effect if the **authentication mode** command is executed. You need to first delete the previous command configuration.

To delete the password, run the **no domain-password** command. If you run the **no domain-password send-only** command, only the **send-only** setting is canceled. If you run the **domain-password psw send-only** and **no domain-password send-only** commands in sequence, the configuration is changed to **domain-password psw**.

Configuration Ruijie(config)# **router isis**

Examples Ruijie(config-router)# **domain-password redgiant**

Related Commands

Command	Description
area-password	Sets the plain-text authentication password of Level-1 area.
authentication mode	Specifies the IS-IS authentication mode.

Platform N/A
Description

4.14 enable mib-binding

Use this command to bind MIBs with an IS-IS process. Use the **no** form of this command to unbind the MIB from the IS-IS process.

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, MIBs are bound with IS-IS process 1.

Command IS-IS routing process configuration mode
Mode

Usage Guide By default, MIBs are bound with IS-IS process 1. The IS-IS process support multiple processes. The administrator can use this command to bind MIBs with the IS-IS process.

Configuration The following example binds the MIB with an IS-IS process.

Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# enable mib-binding
```

Related Commands

Command	Description
graceful-restart helper disable	Disables the IS-IS GR Help capability.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform N/A

Description

4.15 enable traps

Use this command to enable the system to send one or multiple types of IS-IS trap packets. Use the **no** form of this command to disable the system to send IS-IS trap packets.

enable traps { **all** | *traps set* }

no enable traps { **all** | *traps set* }

Parameter Description

Parameter	Description
all	Indicates all types of IS-IS trap packets.
<i>traps set</i>	Indicates the specified type of IS-IS trap packet.

Defaults By default, no IS-IS trap is sent.

Command Mode IS-IS routing process configuration mode

Usage Guide There are 18 types of IS-IS packets. The IS-IS packets can be classified into multiple sets. Each set includes several types of trap packets. To enable the system to send the IS-IS trap packet, you need to enable the global IS-IS trap using the **snmp-server enable traps isis** command, specify the host to receive the IS-IS trap packets, and use the **enable traps** { **all** | *traps set* } command to specify the type of IS-IS trap packet to be sent.

Configuration Examples The following example enables the system to send all IS-IS trap packets to the host of IP address 192.168.1.1.

```
Ruijie# configure terminal
Ruijie(config)#snmp-server enable traps isis
Ruijie(config)#snmp-server host 10.1.1.1 traps version 2c public
```

```
Ruijie(config)#router isis
Ruijie(config-router)# enable traps all
```

**Related
Commands**

Command	Description
graceful-restart helper disable	Disables the IS-IS GR Help capability.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform N/A

Description

4.16 exit-address-family

Use this command to exit IS-IS address family IPv6 configuration mode and return to IS-IS routing process configuration mode.

exit-address-family

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

**Command
Mode** IS-IS address-family IPv6 configuration mode

Usage Guide N/A

Configuration The following example exits IS-IS address family IPv6 configuration mode.

Examples

```
Ruijie (config-router-af)#exit-address-family
Ruijie (config-router)#
```

**Related
Commands**

Command	Description
graceful-restart helper disable	Disables the IS-IS GR Help capability.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform N/A

Description

4.17 graceful-restart

Use this command to enable the IS-IS GR Restart capability. Use the **no** form of this command to disable this capability.

graceful-restart

no graceful-restart

Parameter Description	Parameter	Description
	N/A	N/A

Defaults IS-IS GR is enabled by default.

Command Mode IS-IS routing process configuration mode

Usage Guide Use this command to enable the IS-IS GR Restart capability. As long as the network conditions remain unchanged, IS-IS can be restarted and restored to the pre-restart state without impact on data forwarding.

 The IS-IS GR Restart function is only supported by device which supports hot backup.

Configuration The following example enables the IS-IS GR Restart capability.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# graceful-restart
```

Related Commands	Command	Description
	graceful-restart helper disable	Disables the IS-IS GR Help capability.
	isis hello-interval	Sets the interval of sending Hello packets.
	isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform N/A

Description

4.18 graceful-restart grace-period

Use this command to configure the maximal interval for the graceful-restart. Use the **no** form of this command to restore the default interval.


graceful-restart grace-period *seconds*

no graceful-restart grace-period

Parameter Description	Parameter	Description
		<i>seconds</i>

Defaults The default value is 300 seconds.

Command Mode IS-IS routing process configuration mode

Usage Guide  The IS-IS GR Restart function is only supported by device which supports hot backup.

Configuration Examples The following example sets the interval of the grace-restart to 40 seconds.

```
Ruijie(config)# router isis
Ruijie(config-router)# graceful-restart grace-period 40
```

Related Commands	Command	Description
		graceful-restart
	show isis graceful-restart	Displays the status information of the IS-IS GR Restart.

Platform Description N/A

4.19 graceful-restart helper disable

Use this command to disable the IS-IS GR Helper capability. Use the **no** form of this command to enable this capability.

graceful-restart helper disable
no graceful-restart helper disable

Parameter Description	Parameter	Description
		N/A

Defaults IS-IS GR Helper capacity is enabled by default.

Command Mode IS-IS routing process configuration mode

Usage Guide To disable the IS-IS GR Helper capability, execute this command. In this case, the IS-IS will ignore the request of graceful-restarting the device.

Configuration The following example disables the IS-IS GR Helper capability.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# graceful-restart helper disable
```

Related Commands	Command	Description
		graceful-restart

Platform N/A

Description

4.20 hello padding

Use this command to pad IS-IS Hello packets.

hello padding [multi-point | point-to-point]

Use the **no** form of this command to cancel the padding of IS-IS Hello packets.

no hello padding [multi-point | point-to-point]

Parameter Description	Parameter	Description
		multi-point
	point-to-point	Pads Hello packets of the P2P type.

Defaults Padding is enabled for Hello packets of the LAN type and P2P type by default.

Command Mode IS-IS routing process configuration mode

Default Level 14

Usage Guide Hello packets can be padded to notify a neighbor of the MTU supported by the local device. You can use this command to set whether to pad all Hello packets sent by the IS-IS process. You can also separately specify the type of Hello packets for padding, for example, you can set not to pad all Hello packets of the LAN type or not to pad all Hello packets of the P2P type.

The **isis hello padding** command is available in interface configuration mode. Hello packets sent by a specific interface are not padded if the padding of such Hello packets is cancelled in IS-IS routing process configuration mode or the padding of Hello packets sent by the interface is cancelled in interface configuration mode.

Configuration The following example configures to cancel the padding of Hello packets of the P2P type.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# no hello padding point-to-point
```

4.21 hostname dynamic

Use this command to replace the System ID of the router with the destination router's hostname.

Use the **no** form of this command to cancel this replacement.

hostname dynamic

no hostname dynamic

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the hostname dynamic function is disabled.

Command Mode IS-IS routing process configuration mode

Usage Guide With this command configured, the hostname of the destination router replaces the System ID. The System IDs shown in the execution of the command such as **show isis database**, **show isis neighbors** are all replaced by the hostname of the destination router.

Configuration Ruijie(config)# **router isis**

Examples Ruijie(config-router)# **hostname dynamic**

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.22 ignore-lsp-errors

Use this command to ignore the LSP checksum errors. Use the **no** form of this command to not ignore the LSP checksum errors.

ignore-lsp-errors

no ignore-lsp-errors

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the LSP checksum errors are not ignored.

Command IS-IS routing process configuration mode
Mode

Usage Guide When the local IS-IS receives a LSP, it will calculate the checksum of LSP received and compare the calculated checksum with that in the LSP packets. By default, if the checksum in the LSP packets is different from the checksum calculated, this LSP will be discarded without processing. If we execute the `ignore-lsp-errors` command to ignore the checksum errors, the LSP packets with the incorrect checksum will be processed as the normal packets.

Configuration Ruijie(config) # **router isis**

Examples Ruijie(config-router) # **ignore-lsp-errors**

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

4.23 ip router isis

Use this command to enable the IPv4 IS-IS on the specified interface. Use the **no** form of this command to disable the IPv4 IS-IS routing on the specified interface.

ip router isis [*tag*]

no ip router isis [*tag*]

**Parameter
Description**

Parameter	Description
<i>tag</i>	IS-IS instance name.

Defaults By default, the Ipv4 IS-IS is disabled on the interface.

Command Interface configuration mode
Mode

Usage Guide Use this command to enable the IS-IS IPv4 routing protocol on the interface. The **no** form of this command disables the IS-IS IPv4 routing.
 If the **no ipv4 unicast-routing** is executed in global configuration mode, the IS-IS will disable the IPv4 routing function on all interfaces, namely execute the **no ipv4 router isis** [*tag*] on all interfaces automatically, while other IS-IS configurations will remain unchanged.

Configuration Ruijie(config) # **interface GigabitEthernet 0/1**

Examples Ruijie(config-if) # **ip router isis**

Related Commands	Command	Description
	ipv6 router isis	Enables the IPv6 IS-IS on the interface.
	router isis	Creates IS-IS instances.

Platform N/A
Description

4.24 ipv6 router isis

Use this command to enable the IPv6 IS-IS routing on the specified interface. This command must be configured in the IS-IS configuration. The interface will run on the IS-IS instance named with Tag. If this IS-IS instance is inexistent or this IS-IS instance is not enabled and not initialized, the interface will not enable the IS-IS routing.

Use the **no** form of this command to disable the IPv6 IS-IS routing on the specified interface.

ipv6 router isis [tag]

no ipv6 router isis [tag]

Parameter Description	Parameter	Description
		<i>tag</i>

Defaults By default, the Ipv6 IS-IS routing is not supported on the interface.

Command Mode Interface configuration mode

Usage Guide Configure this command to enable the IS-IS IPv6 routing protocol on the interface. The **no** form of this command disables the IS-IS IPv6 routing.

If the **no ipv6 unicast-routing** is executed in the global configuration mode, the IS-IS will disable the IPv6 routing function on all interfaces, namely execute the **no ipv6 router isis** [tag] on all interfaces automatically, while other IS-IS configurations will remain unchanged.

Configuration Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 router isis
```

Related Commands	Command	Description
	ip router isis	Enables the IPv4 IS-IS on the interface.
	router isis	Creates IS-IS instances.

Platform N/A
Description

4.25 isis authentication key-chain

Use this command to set the key-chain used by the IS-IS interface authentication. Use the **no** form of this command to cancel the specified key-chain.

isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	<i>name-of-chain</i>	Key-chain name with the maximum length being 255.
	level-1	Specifies the authentication key-chain of the Level-1.
	level-2	Specifies the authentication key-chain of the Level-2.

Defaults By default, no IS-IS interface authentication key-chain is specified.

Command Mode Interface configuration mode

Usage Guide If the **key chain** command is not used to configure the corresponding key-chain, the authentication will not be performed. In addition, to make the IS-IS key-chain authentication effective, you need to configure the **isis authentication mode** command at the same time.

This key-chain can apply to the plain-text authentication mode and MD5 encrypted authentication mode. You can use the **isis authentication mode** command to set the authentication mode.

The length of the password key-string in the key-chain shall not be larger than 80 characters if the plain-text authentication mode is used, otherwise this configuration will fail.

Only one key-chain is used at one time. So, when configuring this command, the said key-chain will be overwritten by the new specified one.

If the Level is not specified, the key-chain will apply to both Level-1 and Level-2.

The key-chain specified by this command works on the Hello packets. The IS-IS will send or receive the password that belongs to this key-chain.

There may contain multiple passwords in the key-chain. When sending the packets, use the password with small number first. While receiving the packets, the packet will be received as long as the password of this packet received corresponds to any password in the key-chain.

The authentication commands configured in the IS-IS configuration mode such as authentication key-chain are effective to the LSP, SNP packets, but take no effect on the IS-IS interface.

Configuration Examples The following example specifies the authentication key-chain of the interface GigabitEthernet 0/1 named as *kc*.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis authentication key-chain kc
```

Related Commands	Command	Description
	isis authentication mode	Specifies the mode of IS-IS interface

	authentication.
isis authentication send-only	Specifies the IS-IS interface authentication only applicable to the packets sent, but not to the packets received.
key-chain	Configures the key-chain.

Platform N/A

Description

4.26 isis authentication mode

Use this command to specify the mode of IS-IS interface authentication. Use the **no** form of this command to remove the configuration.

isis authentication mode { md5 | text } [level-1 | level-2]

no isis authentication mode { md5 | text } [level-1 | level-2]

Parameter Description

Parameter	Description
md5	Specifies the MD5 authentication mode.
text	Specifies the plain-text authentication mode.
level-1	Specifies the interface authentication mode to take effect on the Level-1.
level-2	Specifies the interface authentication mode to take effect on the Level-2.

Defaults By default, no interface authentication mode is specified.

Command Mode Interface configuration mode

Usage Guide To make the key-chain configured by the **isis authentication key-chain** command take effect, you must use the **isis authentication mode** command to specify the authentication mode. If the Level is not specified, the authentication mode specified will apply on both Level-1 and Level-2. When configuring the **isis authentication mode** command, if the isis password has been executed, the set command will be overwritten by this command. If the **isis authentication mode** command has been executed, the **isis password** will not be configured successfully. So, you need to delete the **isis authentication mode** command first.

Configuration Examples The following example specifies the authentication mode on the Level-2 of the interface GigabitEthernet 0/1 to be the MD5 authentication mode.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis authentication mode md5 level-2
```

Related Commands	Command	Description
	isis authentication key-chain	Specifies the key-chain used by the IS-IS interface authentication.
	isis authentication send-only	Specifies the IS-IS interface authentication to only apply on the packets sent, but not on the packets received.
	key-chain	Configures the key-chain.
	isis password	Sets the plain-text authentication password for the packets transmit on the IS-IS interface.

Platform N/A

Description

4.27 isis authentication send-only

Use this command to specify the IS-IS interface authentication to only apply to the packets sent and not to the packets received. Use the **no** form of this command to restore the authentication of packets received on the interface.

isis authentication send-only [**level-1** | **level-2**]

no isis authentication send-only [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	level-1	Set the send-only on the Level-1 of the interface.
	level-2	Set the send-only on the Level-2 of the interface.

Defaults By default, this command is not configured. If the IS-IS interface authentication has been configured, then the authentication will be performed on the packets sent and recieved at the same time.

Command Mode Interface configuration mode

Usage Guide With this command configured, the IS-IS will set the authentication password in the Hello packets sent from the interface, however, the authentication will not be performed on the Hello packets received. It can apply to the following two occasions: 1. before deploying the IS-IS interface authentication for all devices in the network. 2. before changing the authentication password or authentication mode. Before the above two tasks start, you need to configure the **isis authentication send-only** command first to make each device perform no authentication on the Hello packets received, so as to avoid the network oscillation caused during the subsequent IS-IS interface authentication deployment. After the deployment of the entire network authentication finished, execute the **no isis authentication send-only** command to cancel the **send-only** authentication mode.

This command can apply to the plain-text authentication mode and MD5 authentication mode. You

can use the **isis authentication mode** command to set the mode used by the IS-IS interface authentication.

If the Level is not specified, the authentication mode specified is applicable to the Level-1 and Level-2.

Configuration Examples The following example specifies the authentication on the Level-1 of the interface GigabitEthernet 0/1 using send-only authentication mode.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis authentication send-only level-1
```

Related Commands

Command	Description
isis authentication key-chain	Specifies the key-chain used by the IS-IS interface authentication.
isis authentication mode	Specifies the mode of the IS-IS interface authentication.
key-chain	Configures the key-chain.

Platform N/A

Description

4.28 isis bfd

Use this command to enable association between IS-IS and BFD on an interface.

isis bfd [disable | anti-congestion]

Use the **no** form of this command to disable association between IS-IS and BFD on an interface.

no isis bfd [disable | anti-congestion]

Parameter Description

Parameter	Description
Disable	Disables association between IS-IS and BFD on an interface.
anti-congestion	Indicates the IS-IS BFD anti-flapping option.

Defaults

If the **bfd all-interfaces** command is configured, association between IS-IS and BFD is enabled on an interface.

If the **bfd all-interfaces** command is not configured, association between IS-IS and BFD is disabled on an interface.

By default, the anti-flapping function is disabled.

Command Mode Interface configuration mode

Default Level 14

Usage Guide

There are two methods for enabling or disabling association between IS-IS and BFD on interfaces.

Method 1: In IS-IS routing process configuration mode, run the [**no**] **bfd all-interfaces [anti-congestion]** command to enable or disable association between IS-IS and BFD on all interfaces running the IS-IS protocol.

Method 2: In interface configuration mode, run the **isis bfd [disable | anti-congestion]** command to enable or disable association between IS-IS and BFD on a specified interface.

In normal cases, the device with the BFD function enabled sends detection packets to detect the link status at an interval of several milliseconds. When a link exception such as link interruption occurs, the device with the BFD function enabled rapidly detects the link exception and informs a device running the IS-IS protocol to delete neighbors and delete neighbor availability information from LSP packets. The device running the IS-IS protocol performs route re-calculation and generates a new route, to bypass the failed link, thereby implementing fast convergence. With the introduction of some new technologies such as the Multi-Service Transport Platform (MSTP), link congestion easily occurs in peak hours. When congestion occurs, the device with the BFD function enabled rapidly detects a link exception, informs a device running the IS-IS protocol to delete a neighbor and delete neighbor availability information from LSP packets, and performs link switching to bypass the congested link. The interval for an IS-IS neighbor to send a Hello detection packet is 10 seconds, and the timeout time is 30 seconds. When an exception is detected via the BFD function, IS-IS Hello packets can be normally received, the IS-IS neighbor relationship can be rapidly reestablished, and the route is restored to pass the congested link. Then, BFD is performed again. If there is still a link exception, link switching is performed repeatedly. The route switches between the congested link and other links and flapping occurs.

The anti-flapping function can be enabled to prevent route flapping in the case of link congestion.

After the anti-flapping function is enabled, if a link is congested, the IS-IS neighbor keeps alive but the neighbor availability information in LSP packets is deleted, and the route switches to a non-congested link. After the link is restored, that is, congestion is eliminated, the neighbor availability information is restored in LSP packets, and the route switches back to the originally congested link, thereby preventing route flapping.

When IS-IS anti-flapping is enabled, the BFD anti-flapping command (**bfd up-dampening**) must be configured on an interface. The two commands must be configured simultaneously. If only one of them is configured, the anti-flapping function does not take effect or a network exception is incurred.

-
- ❓ Before association between IS-IS and BFD is configured, a BFD session must be configured on an interface.
 - ❓ When the BFD anti-flapping command is configured on an interface, if association between IS-IS and BFD is already configured on the interface, the anti-flapping function must be enabled for a device running the IS-IS protocol.
 - ❓ When the IS-IS anti-flapping option is configured, the BFD anti-flapping command must be configured on an interface.
-

Configuration

1. The following example disables association between IS-IS and BFD on GigabitEthernet 0/1.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
```

```
Ruijie(config-if)# no switchport
Ruijie(config-if)# isis bfd disable
```

2. The following example enables the IS-IS BFD anti-flapping option and configures the BFD anti-flapping command on GigabitEthernet 0/1.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# isis bfd anti-congestion
Ruijie(config-if)# bfd up-dampening 60000
```

4.29 isis circuit-type

Use this command to set the circuit-type for the IS-IS interface. Use the **no** form of this command to restore the default settings.

isis circuit-type { level-1 | level-1-2 | level-2-only }

no isis circuit-type

Parameter Description

Parameter	Description
level-1	Forms the Level-1 adjacency.
level-2-only	Forms the Level-2 adjacency.
level-1-2	Forms the Level-1-2 adjacency.
external	Uses the interface as an external domain interface.

Defaults

By default, the circuit-type is Level-1-2.

Command Mode

Interface configuration mode

Usage Guide

If the circuit type is set to Level-1 or Level-2-only, IS-IS will only send PDUs of the corresponding Level.

If the system type is set to Level-1 or Level-2-only, IS-IS only processes the instances of the corresponding Level, and the interface only sends the PDUs of the same Level specified by the **is-type** and **circuit-type** commands.

If the interface is set to **external**, the interface will work as an external domain interface and IS-IS will not send PDUs of the corresponding Level.

Configuration Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis circuit-type level-2-only
```

Related Commands

Command	Description
isis-type	Sets the Level of IS-IS instance.

Platform N/A
Description

4.30 isis csnp-interval

Use this command to set the interval for broadcasting the CSNP packets on the IS-IS interface, with the unit being second. Use the **no** form of this command to restore the default interval.

isis csnp-interval *interval* [**level-1** | **level-2**]

no isis csnp-interval [*interval*] [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	<i>interval</i>	Interval for sending the CSNP packets in the range of 0 to 65535, with the unit being second.
	level-1	Interval for sending the CSNP packets configured only on the Level-1.
	level-2	Interval for sending the CSNP packets configured only on the Level-2.

Defaults By default, in the broadcast network, the interval for sending the CSNP packets is 10 seconds. While in the P2P interface network, no CSNP packet is sent by default.
 When using this command without the parameter Level-1 and Level-2, the new setting is defaulted to be applicable to the Level-1 and Level-2 at the time.

Command Mode Interface configuration mode

Usage Guide Configure this command to change the interval for sending the CSNP packets. By default, the DIS on the broadcast network sends the CSNP packets every 10 seconds.
 For the P2P interface network, by default, the CSNP packets will only be sent at the beginning of adjacency formation. If the interface is set to mesh-groups, you can configure the periodic sending of the CSNP packets.
 If the csnp-interval is set to 0, no CSNP packets will be sent.

Configuration Examples Ruijie(config)# interface GigabitEthernet 0/1

Ruijie(config-if)# isis csnp-interval 20

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.31 isis hello padding

Use this command to specify the filling mode for the IS-IS Hello packets. Use the **no** form of this command to fill no IS-IS Hello packets.

isis hello padding

no isis hello padding

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the **isis hello padding** is executed.

Command Mode Interface configuration mode

Usage Guide Fill the IS-IS Hello packets to advertise the MTU supported to the neighbors. Hello packets can be padded to notify a neighbor of the MTU supported by the local device. In IS-IS routing process configuration mode, the corresponding **hello padding** command also exists. Hello packets sent by a specific interface are not padded if the padding of such Hello packets is cancelled in IS-IS routing process configuration mode or the padding of Hello packets sent by the local interface is cancelled in interface configuration mode.

Configuration The following example fills no IS-IS Hello packets.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# no isis hello padding
```

Related Commands	Command	Description
	isis hello-interval	Sets the interval for sending the Hello packets.

Platform Description N/A

4.32 isis hello-interval

Use this command to set the interval for sending Hello packets on the interface, with the unit being second. Use the **no** form of this command to restore the default interval.

isis hello-interval { *interval* | **minimal** } [**level-1** | **level-2**]

no isis hello-interval [**level-1** | **level-2**]

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>interval</i>	Interval for sending the Hello packet, in the range of 1 to 65536.
minimal	The holdtime is set to the minimal value 1.
level-1	This interval applies on the Level-1.
level-2	This interval applies on the Level-2.

Defaults By default, the interval value is 10 seconds, which is applicable to the Level-1 and Level-2 at the same time.

When using this command without the parameter Level-1 and Level-2, the new setting is defaulted to be applicable to the Level-1 and Level-2 at the time.

Command Mode Interface configuration mode

Usage Guide Configure this command to change the interval for sending Hello packets. By default, the multiplier of the Hello holdtime is 3, and the DIS in broadcast network sends Hello packets at an interval which is three times of non-DIS. If this IS is elected as DIS on this interface, the interface will send Hello packets every 3.3 seconds by default.

If the key word "minimal" is used, then the "holdtime" in Hello packets will be set to 1, and hello interval will be calculated based on the hello-multiplier. For example, if hello-multiplier is configured to 4 and "isis hello-interval minimal" is configured at the same time, the value of hello-interval shall be 1s/4 (250ms).

By default, the CPU protection is enabled on the switch, so that the number of packets corresponding to the destination group addresses of ISIS (AllISSystems, AllL1ISSystems, AllL2ISSystems) is limited when they are sent to the CPU, for example , the default limited value is 400pps. The number of packets received by the switch may be larger than the default value if there are many neighbors or the interval for sending Hello packets is short, resulting in continual vibration of the adjacent relation. In this case, you need to raise the limit of IS-IS packets using the global commands **cpu-protect type isis-is pps**, **cpu-protect type isis-l1is pps** and **cpu-protect type isis-l2is pps**.

Configuration Examples The following example sets the interval for sending Hello packets on the interface.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis hello-interval 5 level-1
```

The following example sets the Holdtime for sending Hello packets on the interface to the minimum value 1.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis hello-interval minimal
```

Related Commands

Command	Description
isis hello-multiplier	Sets the multiplier of the Hello hold timer.

Platform Description N/A

4.33 isis hello-multiplier

Use this command to set the multiplier of Hello hold timer. Use the **no** form of this command to restore the default settings.

isis hello-multiplier *multiplier-number* [**level-1** | **level-2**]

no isis hello-multiplier [*multiplier-number*] [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	<i>multiplier-number</i>	Multiplier value in the range of 2 to 100.

Defaults By default, the multiplier is 3..

Command Mode Interface configuration mode

Usage Guide Use this command to set the multiplier of Hello holdtime. The holdtime value in the Hello packet is the product of hello-interval and this multiplier.

Configuration Ruijie (config) # **router isis**

Examples Ruijie (config-router) # **isis hello-multiplier 5**

Related Commands	Command	Description
	isis hello-interval	Sets the interval for sending the Hello packets.

Platform Description N/A

4.34 isis lsp-interval

Use this command to set the interval for the LSP PDU transmission. Use the **no** form of this command to restore the default interval.

isis lsp-interval *milliseconds* [**level-1** | **level-2**]

no isis lsp-interval [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	<i>milliseconds</i>	Indicates the LSP interval. The value range is 1 to 4,294,967,295, in the unit of milliseconds.
	level-1	Applies the setting only to Level-1 LSPs.
	level-2	Applies the setting only to Level-2 LSPs.

Defaults By default, the lsp-interval is 33ms.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the interval for the LSP PDU transmission to 100.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis lsp-interval 100
```

Related Commands

Command	Description
isis retransmit-interval	Sets the LSP retransmission interval in the P2P network.

Platform N/A

Description

4.35 isis mesh-group

Use this command to add the interface to the specified mesh-group. Use the **no** form of this command to separate the interface from the mesh-group.

isis mesh-group { **blocked** | *mesh-group-id* }

no isis mesh-group

Parameter Description

Parameter	Description
blocked	Blocks all LSP forwarding on the interface.
<i>mesh-group-id</i>	Adds the interface to the mesh-group of specified mesh-group-id with the range being 1 to 4,294,967,295.

Defaults By default, the interface is not added to any mesh-group.

Command Mode Interface configuration mode

Usage Guide Mesh-groups can control the exceeding and redundant LSP spreading in the NBMA network. In the normal condition, the IS-IS router spreads out the LSP from all interfaces except for the receiving one, that is, if a router is configured multiple subinterfaces, the LSP will be sent from all subinterfaces and the neighbors will receive many same LSPs, which wastes a large number of CPU and bandwidth. The IS-IS mesh-group allows grouping the router interfaces, so if a LSP is received by one subinterface in the group, this LSP will not be spread out through other subinterfaces in the group. And if the router receives the LSP from the interface out of the group, it will spread out the LSP from

other interfaces as usual.

If you need to configure the **mesh-group** on the IS-IS interface, use the **isis csnp-interval** command to configure the interval for sending the non-0 CSNP packets, so as to send the CNSP packets regularly to synchronize the LSP and ensure the integrity of LSP synchronization between neighbors in network.

Configuration Ruijie#**configure terminal**
Examples Ruijie(config)# **interface GigabitEthernet 0/1**
 Ruijie(config-if)#**isis mesh-group 1**

**Related
Commands**

Command	Description
isis network point-to-point	Sets the Broadcast interface type of IS-IS to Point-to-Point.

Platform N/A
Description

4.36 isis metric

Use this command to set the metric for the interface. Use the **no** form of this command to restore the default metric.

isis metric *metric* [**level-1** | **level-2**]
no isis metric [*metric*] [**level-1** | **level-2**]

**Parameter
Description**

Parameter	Description
<i>metric</i>	Metric value in the range of 1 to 63.
level-1	Sets this metric to apply on the Level-1 circuit.
level-2	Sets this metric to apply on the Level-2 circuit.

Defaults By default, the metric is 10, which applies on both Level-1 and Level-2 circuit.

**Command
Mode** Interface configuration mode

Usage Guide The Metric value is in the TLV of the IP reachable information and is applied to the SPF calculation. The greater metric value means the more routing cost on this interface and the longer path calculated by SPF.
 This value is effective only when the metric-style includes narrow.

Configuration Ruijie(config)# **interface GigabitEthernet 0/1**
Examples Ruijie(config-if)#**isis metric 1**

Related Commands	Command	Description
	metic-style	Sets the metric type.
	isis wide-metric	Sets the wide metric of the IS-IS interface.

Platform N/A
Description

4.37 isis network point-to-point

Use this command to set the IS-IS Broadcast interface to the Point-to-Point type. Use the **no** form of this command to restore the interface type to the Broadcast.

isis network point-to-point

no isis network point-to-point

Parameter Description	Parameter	Description
		point-to-point

Defaults By default, it is Broadcast type.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis network point-to-point
```

Related Commands	Command	Description
		isis mesh-group

Platform N/A
Description

4.38 isis password

Use this command to set the plain-text authentication password for the Hello packet transmitted on the interface. Use the **no** form of this command to remove the configurations.

isis password *password-string* [**send-only**] [**level-1** | **level-2**]

no isis password [**send-only**] [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	0	Indicates that the key is displayed in plaintext.
	7	Indicates that the key is displayed in ciphertext.
	password-string	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
	send-only	Indicates that the plaintext authentication password is only used to authenticate sent packets. Received packets are not authenticated.
	level-1	Applies the setting to the Level-1 circuit type.
	level-2	Applies the setting to the Level-2 circuit type.

Defaults By default, both the passwords on the Level-1 and Level-2 are not configured.

Command Mode Interface configuration mode

Usage Guide This command is used to set the plain-text authentication password for the Hello packets transmitted on the interface. Use the **no** form of this command to clear the passwords. When the Level is not specified, the authentication password configured is by default applicable to every Level. If the **isis authentication mode** command has been executed, this command will not be configured successfully. To configure this command, you need to delete the **isis authentication mode** command first.

Running the **no isis password send-only** command can only disable the **send-only** option.

Configuration Ruijie(config)# **interface GigabitEthernet 0/1**

Examples Ruijie(config-if)# **isis password redgiant**

Related Commands	Command	Description
	isis authentication mode	Specifies the mode of the IS-IS interface authentication.

Platform N/A

Description

4.39 isis priority

Use this command to set the priority for the DIS election on the LAN. Use the **no** form of this command to restore the default priority.

isis priority *value* [**level-1** | **level-2**]

no isis priority [*value*] [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	<i>value</i>	Value of the priority in the range of 0 to 127.
	level-1	Applies to the Level-1 circuit.
	level-2	Applies to the Level-2 circuit.

Defaults The default priority value is 64 and it is applied on both Level-1 and Level-2 circuit.

Command Interface configuration mode

Mode

Usage Guide Use this command to change the priority value in the Hello of LAN.
 The low priority value has the lower priority in the DIS election than the high priority value.
 This command takes no effect on the Point-to-Point network interface.
 The **no isis priority** command is used to restore the priority to the default value no matter whether the parameter is followed. If you want to modify the configured priority, you can either use the **isis priority** command with *parameter* specified to overwrite the configured command directly, or configure a new parameter after restoring the priority to the default value.

Configuration Ruijie# **configure terminal**

Examples Ruijie(config)# **interface GigabitEthernet 0/1**

Ruijie(config-if)# **isis priority 127 level-1**

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.40 isis psnp-interval

Use this command to set the minimum transmission interval of PSNP packets.

isis psnp-interval *seconds* [**level-1** | **level-2**]

Use the **no** form of this command to cancel the specified minimum transmission interval of PSNP packets.

no isis psnp-interval [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	seconds	Indicates that the value range is 1 to 120 in seconds.
	level-1	Indicates that the configuration takes effect only at Level-1.

level-2	Indicates that the configuration takes effect only at Level-2.
----------------	--

Defaults This command is not configured by default. The default minimum transmission interval is 2 seconds and takes effect both at Level-1 and Level-2.

Command Mode Interface configuration mode

Default Level 14

Usage Guide PSNP packets are used to request for LSP packets or respond to received LSP packets in a point-to-point network. In both cases, it is recommended to send PSNP packets rapidly. If there are excessive LSP packets but the device performance is poor, you can set the PSNP packet transmission interval and LSP retransmission time to larger values, to reduce the device load.

Configuration Examples The following example sets the PSNP packet transmission interval to 5 seconds for Interface GigabitEthernet 0/1 at Level-2.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis psnp-interval 5 level-2
```

4.41 isis retansmit-interval

Use this command to set the LSP retransmission interval. Use the **no** form of this command to restore the default interval.

isis retansmit-interval *seconds* [**level-1** | **level-2**]

no isis retansmit-interval [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	<i>seconds</i>	Indicates the LSP retransmission interval. The value range is 0 to 65,535, in the unit of seconds.
	level-1	Applies the setting only to Level-1 LSPs.
	level-2	Applies the setting only to Level-2 LSPs.

Defaults The default value is 5s.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the LSP retransmission interval. In a P2P network, after a device sends an LSP, if the device receives no PSNP response within the time specified by this command, it will resend the LSP. If the retransmission interval is set to 0, the LSP will not be resent.

The following example sets the LSP retransmission interval to 10s.

Configuration	<code>Ruijie(config)# interface serial 0/1</code>				
Examples	<code>Ruijie(config-if)# isis retransmit-interval 10 level-2</code>				
Related Commands	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #d0d0d0;"> <th style="text-align: left;">Command</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>isis lsp-interval</td> <td>Configures the interval for LSP advertisement on the interface.</td> </tr> </tbody> </table>	Command	Description	isis lsp-interval	Configures the interval for LSP advertisement on the interface.
Command	Description				
isis lsp-interval	Configures the interval for LSP advertisement on the interface.				
Platform	N/A				
Description					

4.42 isis subvlan

Use this command to enable IS-IS on super VLANs. Use the **no** form of this command to restore the default setting.

isis subvlan [**all** | *vid*]

no isis subvlan

Parameter Description	Parameter	Description
	<i>all</i>	Indicates that packets are allowed to be sent to all sub VLANs.
	<i>vid</i>	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults The default setting takes effect only on super VLANs with IS-IS disabled.

Command Interface configuration mode.

Mode

Usage Guide In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when IS-IS multicast packets are sent over a super VLAN containing multiple sub VLANs, the IS-IS multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the IS-IS function does not need to be enabled on a super VLAN. Therefore, the IS-IS function is disabled by default. However, in some scenarios, the IS-IS function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration The following example sends the IS-IS multicast packets to sub VLAN 1024 of super VLAN 300.

Examples	<pre>Ruijie(config)# interface vlan 300 Ruijie(config-if-VLAN 300)# isis subvlan 1024</pre>
-----------------	---

4.43 isis three-way-handshake disable

Use this command to disable three-way handshake for point-to-point network. Use the **no** form of this command to enable three-way handshake for point-to-point network.

isis three-way-handshake disable

no isis three-way-handshake disable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, three-way handshake is enabled.

Command Mode Interface configuration mode

Usage Guide In the point-to-point network, three-way handshake is enabled by default. That is to say, the IS-IS neighbor can be established only after three-way handshake is successful. You can use this command to cancel three-way handshake negotiation to accelerate IS-IS neighbor establishment or for the the device not supporting three-way handshake.

Configuration The following example disables three-way handshake on interface GigabitEthernet 0/0.

```
Ruijie(config)#int GigabitEthernet 0/0
Ruijie(config-if)# isis network point-to-point
Ruijie(config-if)# isis three-way-handshake disable
```

Related Commands	Command	Description
	metric-type	Sets the metric type.
	isis metric	Sets the metric value of the interface.

Platform Description N/A

4.44 isis wide-metric

Use this command to set the wide metric of the interface. Use the **no** form of this command to restore the default wide metric.

isis wide-metric *metric* [**level-1** | **level-2**]

no isis wide-metric [*metric*] [**level-1** | **level-2**]

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>metric</i>	Metric value in the range of 1 to 16,777,241.
level-1	Sets this Metric to apply on the Level-1 circuit.
level-2	Sets this Metric to apply on the Level-2 circuit.

Defaults By default, the metric value is 10 and it is applicable to both Level-1, Level-2 circuit.

Command Mode Interface configuration mode

Usage Guide The Metric value is in the TLV of the IP reachable information and is applied to the SPF calculation. The greater metric value means the more routing cost on this interface and the longer path calculated by SPF.
This value is effective only when the metric-style includes wide.

Configuration Ruijie (config) # **interface GigabitEthernet 0/1**

Examples Ruijie (config-if) #**isis wide-metric 1000**

Related Commands

Command	Description
metric-type	Sets the metric type.
isis metric	Sets the metric value of the interface.

Platform Description N/A

4.45 is-type

Use this command to specify the level for the IS-IS process. Use the **no** form of this command to restore the default level for IS-IS process.

is-type { level-1 | level-1-2 | level-2-only }

no is-type

Parameter Description

Parameter	Description
level-1	Specifies the IS-IS process running on the Level-1 only.
level-1-2	Specifies the IS-IS process running on both Level-1 and Level-2.
level-2-only	Specifies the IS-IS process running on the Level-2 only.

Defaults By default, the IS-IS process runs on Level-1-2.

Command Mode IS-IS routing process configuration mode

Usage Guide Changing the is-type enables or disables the route of one Level.

Configuration Ruijie(config) # **router isis**

Examples Ruijie(config-router) # **is-type level-1**

Related Commands	Command	Description
		isis circuit-type

Platform N/A

Description

4.46 log-adjacency-changes

Use this command to log the changes of the IS adjacency status in case of debug disabled. Use the **no** form of this command to disable this function.

log-adjacency-changes

no log-adjacency-changes

Parameter Description	Parameter	Description
		N/A

Defaults By default, this function is enabled.

Command Mode IS-IS routing process configuration mode

Usage Guide You can also use the **debug** command to log the changes of the IS adjacency status. But using the IS-IS debug command will exhaust large numbers of resources.

Configuration Ruijie(config) # **router isis**

Examples Ruijie(config-router) # **log-adjacency-changes**

Related Commands	Command	Description
		N/A

Platform N/A

Description

4.47 lsp-fragments-extend

Use this command to enable the LSP fragment extension mode for a level. Use the **no** form of this command to disable the LSP fragment extension mode for a level.

lsp-fragments-extend [level-1 | level-2] [compatible rfc3786]

no lsp-fragments-extend [level-1 | level-2] [compatible rfc3786]

Parameter Description	Parameter	Description
	level-1	Enables the LSP fragment extension mode for the Level-1 only.
	level-2	Enables the LSP fragment extension mode for the Level-2 only.
	compatible	Compatible with RFC3786
	rfc3786	The older version of extended LSP implementation.

Defaults By default, LSP fragment extension is disabled.
If no level is specified, the LSP fragment extension mode is enabled for both Level-1 and Level-2.

Command Mode IS-IS routing process configuration mode

Usage Guide The originating LSP can be divided up to 256 fragments. After the 256 fragments are filled, the subsequent link state information, such as the neighbor and IP routing, will be discarded, resulting in network problem.
To avoid the above problem, you can enable the LSP fragment extension function, and configure the additional system ID using the **virtual-system** command.
If there are other vendor's device supporting RFC3786 standard in the network, you need to display the link state database of the device when enabling or disabling the **compatible** option. If there is indeed the vendor's device, you can use the **clear isis *** command to clear the remaining LSP packets to trigger the system to update the link state database.

Configuration Examples The following example enables the LSP fragment extension mode for the Level-2.

```
Ruijie(config)# router isis
Ruijie(config-router)# lsp-fragments-extend level-2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.48 Isp-gen-interval

Use this command to set the minimal interval of the LSP generation. Use the **no** form of this command to restore the default value.

Isp-gen-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval* *hold-interval*]

no Isp-gen-interval [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	level-1	Applies the configuration only to Level-1.
	level-2	Applies the configuration only to Level-2.
	<i>maximum-interval</i>	Indicates the maximum interval for generating two consecutive LSP packets. The value range is 1 to 65535 (in seconds). The default value is 5 .
	<i>initial-interval</i>	Indicates the waiting time for generating an LSP packet for the first time. The value range is 0 to 60000 (in milliseconds). The default value is 50 .
	<i>hold-interval</i>	Indicates the minimum interval for generating an LSP packet for the second time. The value range is 10 to 60000 (in milliseconds). The default value is 200 .

Defaults By default, this command is not configured and the interval of the minimal generation is 5s, it is effective on both Level-1 and Level-2

Command Mode IS-IS routing process configuration mode

Usage Guide The LSP packet generation interval refers to the interval for generating two different LSP packets. A smaller generation interval indicates faster network convergence, which, however, will be accompanied by frequent flooding on the network.

The waiting time for generating an LSP packet for the first time is the initial interval. If the network becomes unstable, the LSP packet regeneration interval is changed to be less than the maximum interval, and the interval for generating an LSP packet for the second time becomes the hold interval. A corresponding penalty will be added to this interval: The next interval for regenerating a LSP packet doubles the previous interval for generating the same LSP packet, until the regeneration interval reaches the maximum interval. Subsequent LSP packets will be generated at the maximum interval. When the network becomes stable, the LSP packet regeneration interval becomes greater than the maximum interval, and the waiting time for LSP packet generation is restored to the initial interval.

Link changes have high requirements for convergence. The initial interval can be set to a small value. The preceding parameters can also be adjusted to larger values to reduce CPU consumption.

The value of **initial-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of **initial-interval** will be used as the value of **maximum-interval**.

The value of **hold-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of **hold-interval** will be used as the value of **maximum-interval**.

The value of **initial-interval** cannot be greater than that of **hold-interval**. Otherwise, the value of **initial-interval** will be used as the value of **hold-interval**.

Configuration Examples The following example sets the minimum interval for generating two duplicate LSP packets to 10 seconds, the interval for generating a duplicate LSP packet for the first time to 100 ms, and the interval for generating a duplicate LSP packet for the second time to 200 ms.

```
Ruijie(config)# router isis
Ruijie(config-router)# lsp-gen-interval 10 100 200
```

The following example sets the minimum interval for generating two duplicate LSP packets to 5 seconds.

```
Ruijie(config)# router isis
Ruijie(config-router)# lsp-gen-interval 5
```

Related Commands

Command	Description
lsp-refresh-interval	Configures the interval for LSP refresh.

Platform N/A
Description

4.49 lsp-length originate

Use this command to set the maximum length for transmitting LSP packets.

lsp-length originate *size* [**level-1** | **level-2**]

Use the no form of this command to restore the default value.

no lsp-length originate [**level-1** | **level-2**]

Parameter Description

Parameter	Description
size	Specifies the maximum length for transmitting LSP packets. The value range is 512 to 16000 in bytes.
level-1	Indicates that the configuration takes effect only at Level-1.
level-2	Indicates that the configuration takes effect only at Level-2.

Defaults The default value of the maximum length for transmitting LSP packets is **1492**. If no level is specified, the default value is **level-1-2**, that is, the configuration takes effect at both Level-1 and Level-2.

Command Mode IS-IS routing process configuration mode

Default Level 14

Usage Guide In principle, the length of LSP and SNP packets cannot be greater than the interface MTU. Otherwise, LSP packets and SNP packets are directly discarded upon being sent.

Configuration The following example sets the maximum length for transmitting LSP packets at Level-2 to 1498 bytes.

Examples

```
Ruijie(config)# router isis 1
Ruijie(config-router)# lsp-length originate 1498 level-2
```

4.50 lsp-length receive

Use this command to set the maximum length for receiving LSP packets.

lsp-length receive *size*

Use the **no** form of this command to restore the default value.

no lsp-length receive

Parameter Description	Parameter	Description
	<i>size</i>	Specifies the maximum length of LSP packets. The value range is 1,492 to 16,000 in bytes according to the RFC.

Defaults The default value is **1492**.

Command Mode IS-IS routing process configuration mode

Default Level 14

Usage Guide This command is used to control the maximum length of LSP packets that can be received by the local device. In fact, to prevent a route convergence failure, intermediate nodes need to receive LSP packets with the maximum length of the interface MTU as long as the memory permits. In this sense, this command seems nominal. The maximum length for receiving LSP packets cannot be less than the maximum length for transmitting LSP packets. If the maximum length for receiving LSP packets is less than the maximum length for transmitting LSP packets, the maximum length for receiving LSP packets is automatically adjusted to the maximum length for transmitting LSP packets.

Configuration The following example configures the maximum length for receiving LSP packets to 1498 bytes.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# lsp-length receive 1498
```

4.51 lsp-refresh-interval

Use this command to set the LSP refresh interval. Use the **no** form of this command to restore the

default value.

lsp-refresh-interval *interval*

no lsp-refresh-interval

**Parameter
Description**

Parameter	Description
<i>interval</i>	LSP refresh interval in the range of 1 to 65535 with unit being second.

Defaults

By default, the lsp-refresh-interval is 900 seconds.

**Command
Mode**

IS-IS routing process configuration mode

Usage Guide

If the LSP stable status lasts for the time of refresh interval, LSP will refresh this LSP and update the LSP version and publish it.

It should be noted that the lsp-refresh-interval must be less than the max lifetime.

Configuration

```
Ruijie(config)# router isis
```

Examples

```
Ruijie(config-router)# lsp-refresh-interval 600
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

4.52 max-area-addresses

Use this command to set the maximal number of area address allowed. Use the **no** form of this command to restore the default value.

max-area-addresses *value*

no max-area-addresses

**Parameter
Description**

Parameter	Description
<i>value</i>	The maximal number of area address allowed, in the range of 3 to 6.

Defaults

By default, the max-area-addresses is 3.

**Command
Mode**

IS-IS routing process configuration mode

Usage Guide

For the IS routers of Level-1, only the ones with the same max-area-addresses are allowed to establish the adjacency relation.

Configuration Ruijie(config)# **router isis**

Examples Ruijie(config-router)# **max-area-addresses 5**

**Related
Commands**

Command	Description
net	Sets the IS-IS NET(Network Entry Title) address.

Platform N/A

Description

4.53 maximum-paths

Use this command to set the maximum number of IS-IS equal-cost routing entries in the routing table.

maximum-paths *maximum*

Use the **no** form of this command to restore the default value.

no maximum-paths

**Parameter
Description**

Parameter	Description
<i>maximum</i>	Maximum number of IS-IS equal-cost routing entries in the routing table. The value range is 1 to 32 .

Defaults The default value is **2**.

Command Mode IS-IS routing process configuration mode, IS-IS address-family IPv6 configuration mode

Default Level 14

Usage Guide This command is used by the IS-IS protocol to control the number of IS-IS equal-cost routing entries in the routing table. The routing table itself also has a command for controlling the number of equal-cost routing entries. The effective number of equal-cost routing entries is the smaller of the two values.

Configuration Examples The following example sets the maximum number of IS-IS IPv4 equal-cost routing entries in the routing table to **5**.

```
Ruijie(config)# router isis
Ruijie(config-router)# maximum-paths 5
```

The following example sets the maximum number of IS-IS IPv6 equal-cost routing entries in the routing table to **6**.

```
Ruijie(config)# router isis
```

```
Ruijie(config-router)# address-family ipv6
Ruijie(config-router-af)# maximum-paths 6
```

4.54 max-lsp-lifetime

Use this command to set the maximum value of the LSP lifetime. Use the **no** form of this command to restore the default value.

max-lsp-lifetime *value*

no max-lsp-lifetime

Parameter Description

Parameter	Description
<i>value</i>	Maximum value of the LSP lifetime in the range of 1 to 65,535, with unit being second.

Defaults By default, the max-lsp-lifetime is 1200 seconds.

Command Mode IS-IS routing process configuration mode

Usage Guide It should be noted that the max-lsp-lifetime must be greater the lsp-refresh-interval.

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# max-lsp-lifetime 1500
```

Related Commands

Command	Description
lsp-refresh-interval	Configures the interval for LSP refresh.

Platform Description N/A

4.55 metric-style

Use this command to set the metric style. Use the **no** form of this command to restore the default metric style.

metric-style { **narrow** [**transition**] | **wide** [**transition**] | **transition** } [**level-1** | **level-1-2** | **level-2** |]

no metric-style { **narrow** [**transition**] | **wide** [**transition**] | **transition** } [**level-1** | **level-1-2** | **level-2** |]

Parameter Description

Parameter	Description
-----------	-------------

narrow	Uses the old metric style with the router interface metric ranging from 1 to 63.
wide	Uses the new metric style with the router interface metric ranging from 1 to 16777214
transition	Allows the router to send and receive the new and old metric style.
level-1	This metric-style on the Level-1 circuit.
level-2	This metric-style applies on the Level-2 circuit.
level-1-2	This metric-style applies on the Level-1-2 circuit.

Defaults By default, the metric-style is narrow.

Command IS-IS routing process configuration mode

Mode

Usage Guide The metric value of the interface is specified by the **isis metric** *metric* when the metric-style is set to narrow, while the metric value is specified by the **isis wide-metric** *metric* in case that the metric-style is set to wide or **transition**.

Configuration Ruijie(config) # **router isis**

Examples Ruijie(config-router) # **metric-style wide**

**Related
Commands**

Command	Description
isis metric	Sets the metric of the interface.
isis wide-metric	Sets the wide metric of the interface.

Platform N/A

Description

4.56 multi-topology

Use this command to enable IS-IS to support IPv6 unicast topology. Use the **no** form of this command to restore the default setting.

multi-topology [transition]

no multi-topology [transition]

**Parameter
Description**

Parameter	Description
transition	Configures the MT transition mode.

Defaults By default, multitopology is not configured, namely, IS-IS does not support IPv6 unicast topology.

Command IS-IS address-family IPv6 configuration mode

Mode

- Usage Guide**
1. When this command is not configured, IPv4 and IPv6 share the same IS-IS physical topology, which is also called default topology.
 2. If the **transition** parameter is not specified, the device runs in multi-topology mode, the IS-IS v4 process works in the default topology while the IS-IS v6 process works in the IPv6 unicast topology.
 3. If the **transition** parameter is specified, the device runs in multi-topology transition mode and the IS-IS v6 process runs in both the default topology and IPv6 unicast topology.

The above three configurations are exclusive.

The device which runs in multi-topology transition mode can transmit the multi-topology TLV and the default topology TLV. The multi-topology transition mode can be applied in incremental deployment to ensure smooth network migration. However, this mode may cause leaking of routes between the default topology and IPv6 unicast topology. Be careful to configure multi-topology transition mode, as this configuration may lead to network problems such as route blackhole and network loop.

Before you configure this command, you need to set the metric style as wide or transition mode.

Configuring the metric style as narrow and configuring only one Level to support wide or transition mode will disable the multitopology routing (MTR) function.

Configuration The following example configures multi-topology.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# address-family ipv6
Ruijie(config-router-af)# multi-topology
```

Related Commands

Command	Description
router isis	Creates IS-IS instances.

Platform

N/A

Description**4.57 net**

Use this command to set the IS-IS NET (Network Entry Title) address. Use the **no** form of this command to delete this NET address.

net *net-address*

no net *net-address*

Parameter Description

Parameter	Description
<i>net-address</i>	The format of net-address is shown as below: XX..XXXX.YYYY.YYYY.YYYY.00, the XX...XXXX is the area address and the YYYY.YYYY.YYYY is the system ID.

Defaults By default, no NET address is set.

Command Mode IS-IS routing process configuration mode

Usage Guide This command is used to set the Area ID and System ID for the IS-IS. Up to three NET addresses are allowed to be set by default, namely three addresses with different Area can be set. However, the System ID must be the same.

Configuration Ruijie(config)# **router isis**

Examples Ruijie(config-router)# **net** 49.0000.0001.0002.0003.00

Related Commands	Command	Description
		router isis

Platform N/A

Description

4.58 passive-interface

Use this command to configure the passive interface. Use the **no** form of this command to remove the passive interface.

passive-interface [**default**] { *interface-type interface-number* }

no passive-interface [**default**] { *interface-type interface-number* }

Parameter Description	Parameter	Description
		default
	<i>interface-type</i>	Indicates the interface type.
	<i>interface-number</i>	Indicates the interface number.

Defaults The passive interface is not configured by default.

Command Mode IS-IS routing process configuration mode

Usage Guide Use this command to disable the interface to receive and send the IS-IS packets, but to advertise the IP address of the interface.

After the **default** option is configured, if the number of IS-IS disabled interfaces exceeds 255, the first 255 interfaces are configured as passive and the remaining interfaces are non-passive.

Configuration The following example configures interface GigabitEthernet 0/0 as passive.

Examples Ruijie(config)# **router isis** 1

```
Ruijie(config-router)# passive-interface GigabitEthernet 0/0
```

Related Commands

Command	Description
router isis	Creates IS-IS instances.

Platform N/A

Description

4.59 redistribute

Use this command to redistribute the routes from one routing protocol into another routing protocol.

Use the **no** form of this command to delete the redistribution.

```
redistribute { bgp | ospf process-id match { internal | external [ 1 | 2 ] | nssa-external [ 1 | 2 ] } |
rip | connected | static } [ metric metric-value ] [ metric-type type-value ] [ route-map map-tag ]
[ level-1 | level-1-2 | level-2 ]
no redistribute { bgp | ospf process-id [ match { internal | external [ 1 | 2 ] | nssa-external [ 1 |
2 ] } ] | rip | connected | static } [ metric metric-value ] [ metric-type { internal | external } ]
[ route-map map-tag ] [ level-1 | level-1-2 | level-2 ]
```

Parameter Description

Parameter	Description
<i>process-id</i>	OSPF process ID, in the range of 1 to 65535.
match { internal external [1 2] nssa-external [1 2] }	Redistributes the OSPF routes to perform the filtering on the subtype of the OSPF routes. If the match option is not specified, all routes of the ospf subtype by default are received. If the 1 or 2 followed by the match external is not specified, then redistribute the route of the OSPF external1 and external 2 . if the 1 or 2 following the match nssa-external is not specified, then redistribute the routes of OSPF nssa-external 1 and nssa-external 2 .
metric <i>metric-value</i>	Sets the metric value of redistributing the route, in the range of 0 to 4261412864. If the metric option is not specified, the external metric value is used.
metric-type { internal external }	Sets the metric type of redistributing the route. internal : use the internal metric type. external : use the external metric type. If the metric-type is not specified, the internal type is used by default.
route-map <i>map-tag</i>	Sets the route-map during the external routes redistribution, which is used to filter the redistributed routes or set attributions of the routes. The name of <i>map-tag</i> shall not be over 32 characters. No route-map is configured by default.
level-1 level-1-2 level-2	Specifies the Level of receiving the redistributed routing information. If the Level is not specified, it is defaulted to be redistributed into the Level-2 .

The format is shown as below:

level-1: redistribute into the Level-1

level-1-2: redistribute into both Level-1 and Level-2.

level-2: redistribute into the Level-2.

Defaults By default, no redistribution is configured.

Command IS-IS routing process configuration mode , IS-IS address-family ipv6 mode

Mode

Usage Guide Configure "**no redistribute { bgp | ospf processs-id | rip | connected | static }**" to disable protocol redistribution. If "**no redistribute**" is followed by any other parameter, it means that this parameter is restored to the default setting instead of disabling protocol redistribution. For example: "**no redistribute bgp**" will disable bgp redistribution, while "**no redistribute bgp route-map aa**" will disable route-map aa filtering during redistribution instead of disabling bgp redistribution.

The routing information will be placed into the IP External Reachability Information TLV of LSP when redistributing external route in the IPv4 mode.

The routing information will be placed to the IPv6 Reachable TLV of LSP when redistributing external route in the IPv6 mode.

In the old version of some vendors, after configuring the **metric-type** to the **external**, the redistributed route metric will be added by 64 and then perform the routing according to the metric value during the routing calculation, which violates the protocol. In actual application, the priority of the external route may be higher than that of the internal route. When connecting with these old version of some vendors, the related configuration (such as the **metric** or the **metric-type**) of each device can be modified to ensure that the priority of the internal route is higher than the external.

The following example sets the metric value to 10.

Configuration Ruijie(config)# **router isis**

Examples Ruijie(config-router)# **redistribute ospf 1 metric 10 level-1**

**Related
Commands**

Command	Description
redistribute isis [tag] level-2 into level-1	Redistributes the reachable routing information from Level-2 into Level-1.
redistribute isis [tag] level-1 into level-2	Redistributes the reachable routing information from Level-1 into Level-2.
route-map	Configures the route map.

Platform N/A

Description

4.60 redistribute isis level-1 into level-2

Use this command to redistribute the Level-1 reachable routing information of the IS-IS instance into

the Level-2 of current instance. Use the **no** form of this command to disable this redistribution.

redistribute isis [*tag*] **level-1 into level-2** [**route-map** *route-map-name* | **distribute-list** *access-list-name*]

no redistribute isis [*tag*] **level-1 into level-2** [**route-map** *route-map-name* | **distribute-list** *access-list-name*]

Parameter Description

Parameter	Description
<i>tag</i>	Name of the IS-IS instance.
route-map <i>route-map-name</i>	Sets the route map during the route redistribution, which is used to filter the redistributed route and set attributions of this route. Name of the <i>route-map-name</i> shall not be over 32 characters. No route-map is configured by default.
distribute-list <i>access-list-name</i>	Uses the distribute-list to filter the redistributed routes. Access-list-name is the prefix list associated, it can be the standard, extended or naming prefix list. The format is shown as below: {<1-99> <100-199> <1300-1999> <2000-2699> <i>acl-name</i> } In the IS-IS address-family ipv6 mode, you can use only the naming prefix list with the format being <i>acl-name</i> .

Defaults


If the IS-IS Level-2 instance exists, all IS-IS Level-1 routes are by default redistributed into the IS-IS Level-2 instance.

Command Mode

IS-IS routing process configuration mode or IS-IS **address-family ipv6** mode.

Usage Guide

Use the **route-map** or **distribute-list** to filter the Level-1 route of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into the Level-1 of current instance.

 You can only choose one of the two parameters **route-map** and **distribute-list**.

Configure the **no distribute isis** [*tag*] **level-2 into level-1** to disable the specified instance redistribution. If the **no redistribute** is followed by any other parameters, it means that this parameter is restored to the default setting instead of disabling the specified instance redistribution.

For example: "**no redistribute isis tag1 level-1 into level-2**" will disable the isis tag1 redistribution, while "**no redistribute isis tag1 level-1 into level-2 route-map aa**" will disable route-map aa filtering during redistribution instead of disabling the isis tag1 redistribution.

Configuration

```
Ruijie(config)# router isis aa
```

Examples

```
Ruijie(config-router)# redistribute isis bb level-1 into level-2
```

Related Commands

Command	Description
redistribute	Redistributes the routing information from

	another routing protocol.
redistribute isis level-2 into level-1	Redistributes the reachable routing information from Level-2 into Level-1.

Platform N/A

Description

4.61 redistribute isis level-2 into level-1

Use this command to redistribute the Level-2 reachable routing information of the IS-IS instance into the Level-1 of current instance. Use the **no** form of this command to remove the redistribution.

redistribute isis [*tag*] **level-2 into level-1** [**route-map** *route-map-name* | **distribute-list** *access-list-name*] (**prefix** *ip-address net-mask* | **ipv6-prefix** *ipv6-address/length*)

no redistribute isis [*tag*] **level-2 into level-1** [**route-map** *route-map-name* | **distribute-list** *access-list-name*] (**prefix** *ip-address net-mask* | **ipv6-prefix** *ipv6-address/length*)

Parameter Description

Parameter	Description
<i>tag</i>	Name of the IS-IS instance to be redistributed.
route-map <i>route-map-name</i>	Sets the route map during the route redistribution, which is used to filter the redistributed routes and set attributions of the routes. Name of the <i>route-map-name</i> shall not be over 32 characters. <ul style="list-style-type: none"> No route-map is configured by default.
distribute-list <i>access-list-name</i>	<ul style="list-style-type: none"> Uses the distribute-list to filter the redistributed routes. Access-list-name is the prefix list associated, it can be the standard, extended or naming prefix list. The format is shown as below: <ul style="list-style-type: none"> {<1-99> <100-199> <1300-1999> <2000-2699> <i>acl-name</i>} In the IS-IS address-family ipv6 mode, you can use only the naming prefix list with the format being <i>acl-name</i>.

Defaults N/A

Command Mode IS-IS routing process configuration mode or IS-IS **address-family ipv6** mode.

Usage Guide Use the **route-map** or **distribute-list** to filter the Level-2 route of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into the Level-1 of current instance.

 You can only choose one of the two parameters **route-map** and **distribute-list**.

Configure the **no distribute isis** [*tag*] **level-2 into level-1** to disable the specified instance redistribution. If the **no redistribute** is followed by any other parameters, it means that this parameter is restored to the default setting instead of disabling the specified instance redistribution.

For example: "**no redistribute isis tag1 level-2 into level-1**" will disable the isis *tag1* redistribution, while "**no redistribtue isis tag1 level-2 into level-1 route-map a**" will disable route-map *aa* filtering during redistribution instead of disabling the isis *tag1* redistribution.

Configuration Ruijie(config)# router isis aa

Examples Ruijie(config-router)# redistribute isis bb level-2 into level-1

**Related
Commands**

Command	Description
redistribute	Redistributes the routing information from another routing protocol.
redistribute isis level-1 into level-2	Redistributes the reachable routing information from Level-1 into Level-2.

Platform N/A

Description

4.62 router isis

Use this command to create the IS-IS instance. Use the **no** form of this command to delete this instance.

router isis [*tag*]

no router isis [*tag*]

**Parameter
Description**

Parameter	Description
<i>tag</i>	Instance name

Defaults By default, no IS-IS instance is configured.

**Command
Mode** Global configuration mode

Usage Guide Use this command to initialize the IS-IS instance and enter the IS-IS routing process configuration mode.

The IS-IS instance will not be executed unless one NET address is configured at least.

When enabling the IS-IS routing process with the parameter *tag*, the parameter *tag* will be used as well when disabling the IS-IS routing process.

By default, the CPU protection is enabled on the switch, so that the number of packets corresponding to the destination group addresses of ISIS (AllISSystems, AllL1ISSystems, AllL2ISSystems) is limited when they are sent to the CPU, for example , the default limited value is 400pps. The number of packets received by the switch may be larger than the default value if there are many neighbors or the interval for sending Hello packets is short, resulting in continual vibration of the adjacent relation. In this case, you need to raise the limit of IS-IS packets using the global commands **cpu-protect type**

isis-is pps, **cpu-protect type isis-l1is pps** and **cpu-protect type isis-l2is pps**.

Configuration Ruijie# **configure terminal**
Examples Ruijie(config)# **router isis**

Related Commands	Command	Description
	ip router isis	Enables the IS-IS IPv4 routing protocol on the interface.
	ipv6 router isis	Enables the IS-IS IPv6 routing protocol on the interface.
	net	Sets the NET address.

Platform N/A
Description

4.63 set-overload-bit

Use this command to instruct a neighbor not to use the local IS-IS node as a transit device for forwarding data.

set-overload-bit [**on-startup** *seconds*] [**suppress** { [**interlevel**] [**external**] }] [**level-1** | **level-2**]

Use the **no** form of this command to disable the function of instructing a neighbor not to use the local IS-IS node as a transit device for forwarding data.

no set-overload-bit [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	on-startup <i>seconds</i>	Indicates that an IS-IS node automatically enters the OVERLOAD state after restart. seconds is the duration of the IS-IS node in the OVERLOAD state after restart. The value range is 5 to 86,400 in seconds.
	suppress	Indicates that internal routes (IS-IS inter-area routes and intra-area routes) or external routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state.
	interlevel	Indicates that IS-IS inter-area routes and intra-area routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state. It is used in combination with the suppress keyword.
	external	Indicates that external routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state. It is used in combination with the suppress keyword.
	level-1	Sends LSP packets that carry the OVERLOAD bit only to Level-1 neighbors.

level-2	Sends LSP packets that carry the OVERLOAD bit only to Level-2 neighbors.
----------------	--


Defaults The function of instructing a neighbor not to use the local IS-IS node as a transit device for forwarding data is disabled by default.

Command Mode IS-IS routing process configuration mode

Default Level 14

Usage Guide This command forces a IS-IS node to set the OVERLOAD bit in non-virtual LSP packets, to instruct IS-IS neighbors not to use the local node as a transit device.

If the **on-startup** keyword is carried, the device automatically enters the OVERLOAD state after restart. If the **on-startup** keyword is not carried, the device immediately enters the OVERLOAD state upon restart.

 The **on-startup** keyword takes effect for only one level.

The OVERLOAD bit is mainly used in the following cases:

- Device overload

The overload of the local IS-IS node, for example, memory insufficiency or CPU full load, may cause incomplete routes in the local routing table or no resource for data forwarding. You can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local node as a transit device.

In this case, the **on-startup** keyword is not carried in the configuration. The OVERLOAD bit is manually set or cancelled. You must manually cancel this command after the local IS-IS node restores to the normal state. Otherwise, the local IS-IS node is always in the OVERLOAD state

- Instantaneous black hole

In the scenario described in RFC3277, the IS-IS converges faster than BGP does. After an IS-IS node restarts, the route fails instantaneously, that is, instantaneous black hole occurs. You can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local node as a transit device till the specified timer expires.

In this case, the configuration must carry the **on-startup** field. The OVERLOAD bit is automatically set or cancelled by the IS-IS node based on the configuration.

After the **on-startup** field is selected, the IS-IS node automatically enters the instantaneous black hole state after restart. After a new neighbor relationship is established, the IS-IS node immediately sends the LSP packet that carries the OVERLOAD bit to notify the neighbor that the local device enters the instantaneous black hole state (or OVERLOAD state) and that the local node cannot be used as a transit device.

When the specified timer expires, the IS-IS node immediately sends the LSP packet without the OVERLOAD bit to notify the neighbor that the local device is no longer in the instantaneous state (or OVERLOAD state) and can be used as a transit device.

The timer time needs to be set based on the number of routes in the network. If there are many routes, set it to a large value; if there are a few routes, set it to a small value.

- The local IS-IS node is not intended to be used for forwarding real data

If the local IS-IS node needs to be connected to the production network for testing or other function requirements and it is not intended to be used for forwarding real data in the network, you can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local device as a transit device.

In this case, the **on-startup** field is not carried in the configuration and the OVERLOAD bit is manually set or cancelled.

You can configure **suppress** as required to restrict the routing information carried in LSP packets in the OVERLOAD state, for example, suppress internal routes and external routes and advertise only local direct routes.

Configuration Examples The following example sets an IS-IS node to immediately enter the instantaneous black hole state after restart till the specified timer expires (set the specified waiting time to 300 seconds) and advertises only local direct routes to neighbors.

```
Ruijie(config)# router isis
Ruijie(config-router)#set-overload-bit on-startup 300 suppress interlevel
external
```

The following example connects the local IS-IS node to the production network as a test device and set its not to forward real data of the production network, to avoid impact on production.

```
Ruijie(config)# router isis
Ruijie(config-router)#set-overload-bit suppress interlevel external
```

4.64 show clns is-neighbor

Use this command to display all IS neighbors to provide the adjacency relationship of routers.

show clns [tag] is-neighbors [interface-type interface-number] [detail]

Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.
	<i>interface-type</i> <i>interface-number</i>	Specifies the name of interface.
	detail	Displays detailed information of all interfaces.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide N/A

Configuration Examples The output results of the **show clns is-neighbors detail** command are displayed as below:

```
Area (null):
```

```

System Id  Type  IP Address  State  Holdtime  Circuit  Interface
r1         L1    1.0.0.2    Up     9         r1.01    VLAN 1
L2    1.0.0.2    Up     9         r1.01    VLAN 1

Adjacency ID: 1
Uptime: 00:00:54
Area Address(es): 49.1111
IP Address(es): 1.0.0.2
Level-1 Protocols Supported: IPv4
Level-2 Protocols Supported: IPv4

```

**Related
Commands**

Command	Description
show clns neighbors	Displays all IS neighbors to provide the router information and the adjacency relationship of terminal system.

Platform N/A**Description**

4.65 show clns neighbors

Use this command to display all IS neighbors to provide the router information and the adjacency relationship of terminal system.

show clns [*tag*] **neighbors** [*interface-type interface-number*] [**detail**]

**Parameter
Description**

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.
<i>interface-type</i> <i>interface-number</i>	Specifies the name of the interface.
detail	Displays detailed information of all interfaces.

Defaults N/A**Command
Mode** Privileged EXEC mode, global configuration mode or interface configuration mode.**Usage Guide** N/A**Configuration
Examples** The following example displays all IS neighbors to provide the router information and the adjacency relationship of terminal system.

```

Ruijie# show clns neighbors detail

Area (null):

```

```

System Id      SNPA                State Holdtime  Type Protocol Interface
r1             00d0.f8bc.de08     Up    7         L1  IS-IS   GigabitEthernet 0/0
                                             Up    9         L2  IS-IS   GigabitEthernet 0/0

Adjacency ID: 1
Uptime: 00:01:40
Area Address(es): 49.1111
IP Address(es): 1.0.0.2
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
Level-2 MTID: Standard
Level-1 Protocols Supported: IPv4, IPv6
Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up

```

**Related
Commands**

Command	Description
show clns is-neighbors	Displays all IS neighbors to provide the router adjacency relationship.

Platform N/A
Description

4.66 show isis counter

Use this command to display various statistics of IS-IS.

show isis [tag] counter

**Parameter
Description**

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide N/A

Configuration Examples The output results of the **show clns neighbors details** are displayed as below:

```

Ruijie# show isis counter
Area (null):
IS-IS Level-1 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0

```

```
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 30
IS-IS Level-2 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 30
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

4.67 show isis database

Use this command to display the LSP database.

show isis [tag] database [FLAGS | LEVEL | LSPID]

Parameter Description

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.
<i>FLAGS</i>	The format is displayed as below: detail verbose detail: detailed information

	Verbose: more detailed information than the detail.
<i>LEVEL</i>	The format is displayed as below: l1 l2 level-1 level-2 l1 and level-1: specify the LSP database of the Level-1. l2 and level-2: specify the LSP database of the Level-2
<i>LSPID</i>	Specifies the ID number of LSP to show the corresponding LSP information only.
<i>tag</i>	Specifies the IS-IS instance.

Defaults N/A

Command Privileged EXEC mode, global configuration mode or interface configuration mode.

Mode

Usage Guide N/A

Configuration The output results of the **show isis database detail** command are displayed as below:

Examples

```
Ruijie# show isis database detail
Area (null):
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Ruijie.00-00 * 0x00000007  0xCDD5        1011          0/0/0
  Area Address: 49.1111
  NLPID:        0xCC
  Hostname:     Ruijie
  IP Address:   1.0.0.1
  Metric: 10    IS r1.01
  Metric: 10    IP 1.0.0.0 255.255.255.0
r1.00-00       0x00000006  0xA771        1032          0/0/0
  Area Address: 49.1111
  NLPID:        0xCC
  Hostname:     r1
  IP Address:   1.0.0.2
  Metric: 10    IS r1.01
  Metric: 10    IP 1.0.0.0 255.255.255.0
r1.01-00       0x00000002  0x062A        989           0/0/0
  Metric: 0     IS r1.00
  Metric: 0     IS Ruijie.00

IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Ruijie.00-00 * 0x0000000A  0xC7D8        1033          0/0/0
  Area Address: 49.1111
  NLPID:        0xCC
```

```

Hostname:    Ruijie
IP Address:  1.0.0.1
Metric:     10          IS r1.01
Metric:     10          IP 1.0.0.0 255.255.255.0
r1.00-00    0x00000006  0xA771          1032          0/0/0
Area Address: 49.1111
NLPID:      0xCC
Hostname:    r1
IP Address:  1.0.0.2
Metric:     10          IS r1.01
Metric:     10          IP 1.0.0.0 255.255.255.0
r1.01-00    0x00000002  0x062A          989           0/0/0
Metric:     0          IS r1.00
Metric:     0          IS Ruijie.00

```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

4.68 show isis graceful-restart

Use this command to display the status information related to the IS-IS GR.

show isis [tag] graceful-restart

**Parameter
Description**

Parameter	Description
tag	IS-IS instance name

Defaults N/A

Command Mode Privileged EXEC mode/ global configuration mode/ interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the GR information of the IS-IS.

```

Ruijie(config)# show isis graceful-restart

Area (null):
Graceful-restart Helper: enabled
Level 1:

```



```
GigabitEthernet 0/0: RR received: 0
Level 2:
GigabitEthernet 0/0: RR received: 0
Graceful-restart: enabled
Graceful-period: 400s, Level timer: 60s, Interface timer: 3s
Instance GR status: not restarting
```

**Related
Commands**

Command	Description
graceful-restart	Enables the IS-IS GR Restart capability.
graceful-restart grace-period	Configures the maximum interval of the grace-restart.
graceful-restart helper disable	Disables the IS-IS GR Help capability.
graceful-restart	Enables the IS-IS GR Restart capability.

Platform N/A**Description**

4.69 show isis hostname

Use this command to display the mapping relation between the router name and system ID.

show isis [tag] hostname

**Parameter
Description**

Parameter	Description
<i>tag</i>	Specifies the IS-IS instance.

Defaults N/A**Command
Mode** Privileged EXEC mode/ global configuration mode/ interface configuration mode**Usage Guide** N/A**Configuration****Examples**

```
Ruijie# show isis hostname

System ID      Dynamic Hostname      Area (null)
* 5555.5555.5555 Ruijie
  1111.1111.1111 R1

System ID      Dynamic Hostname      Area 1
* 4444.4444.4444 Ruijie
  2222.2222.2222 R2
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.70 show isis interface

Use this command to display the information about IS-IS interface.

show isis [*tag*] **interface** [*interface-type interface-number*] [*counter*]

Parameter Description	Parameter	Description
	<i>tag</i>	
<i>interface-type</i> <i>interface-number</i>		Specifies the Interface name.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the IS-IS interface.

```
Ruijie# show isis interface
Area (null):
VLAN 1 is up, line protocol is up
  Routing Protocol: IS-IS ((null))
    Network Type: Broadcast
    Circuit Type: level-1-2
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000001
    Local SNPA: 00d0.f822.33ab
    IP interface address:
      1.0.0.1/24
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: r1.01
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10/10, Priority: 64, Circuit ID: r1.01
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 5 seconds
    Next IS-IS LAN Level-2 Hello in 5 seconds
```

```

BFD Enabled (Anti-congestion)
Eligible to backup traffic
FRR Protect Enabled (Link)

```

The following example displays the statistics of the IS-IS interface.

```

Ruijie# show isis interface counter

Area (null):
GigabitEthernet 1/1/0:
  IS-IS LAN Level-1 isisCircuitCounterEntry:
    isisCircAdjChanges: 4
    isisCircNumAdj: 2
    isisCircInitFails: 0
    isisCircRejAdjs: 0
    isisCircIDFieldLenMismatches: 0
    isisCircMaxAreaAddrMismatches: 0
    isisCircAuthTypeFails: 0
    isisCircAuthFails: 0
    isisCircLanDesISChanges: 1
  IS-IS LAN Level-2 isisCircuitCounterEntry:
    isisCircAdjChanges: 4
    isisCircNumAdj: 2
    isisCircInitFails: 0
    isisCircRejAdjs: 0
    isisCircIDFieldLenMismatches: 0
    isisCircMaxAreaAddrMismatches: 0
    isisCircAuthTypeFails: 0
    isisCircAuthFails: 0
    isisCircLanDesISChanges: 1
  IS-IS Level-1 isisPacketCounterEntry:
    isisPacketCountIIHello in/out: 187/278
    isisPacketCountLSP in/out: 10/7
    isisPacketCountCSNP in/out: 0/92
    isisPacketCountPSNP in/out: 0/0
    isisPacketCountUnknown in/out: 0/0
  IS-IS Level-2 isisPacketCounterEntry:
    isisPacketCountIIHello in/out: 186/286
    isisPacketCountLSP in/out: 17/9
    isisPacketCountCSNP in/out: 1/91
    isisPacketCountPSNP in/out: 0/0
    isisPacketCountUnknown in/out: 0/0

```

**Related
Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

Platform N/A

Description

4.71 show isis ipv6 topology

Use this command to display information about the IPv6 unicast topology to which an IS-IS router is connected.

show isis [tag] ipv6 topology [I1 | I2 | level-1 | level-2]

Parameter Description	Parameter	Description
	<i>tag</i>	IS-IS instance
	I1	Topology of a specified Level-1 router
	level-1	Topology of a specified Level-1 router
	I2	Topology of a specified Level-2 router
	level-2	Topology of a specified Level-2 router

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example displays the IPv6 unicast topology information.

```
Ruijie#show isis ipv6 topology
Area (null):
IS-IS paths to level-1 routers
System Id   Metric   Next-Hop   SNPA           Interface
r1          10      r1         00d0.f822.33ad GigabitEthernet 0/0
Ruijie      --
IS-IS paths to level-2 routers
System Id   Metric   Next-Hop   SNPA           Interface
r1          10      r1         00d0.f822.33ad GigabitEthernet 0/0
Ruijie      --
```

Field description:

Field	Description
Area	Instance tag
System Id	System ID
Metric	Metric value
Next-Hop	Next hop

SNPA	SNPA address
Interface	Interface name

4.72 show isis mesh-groups

Use this command to display the mesh-group configurations on each interface.

show isis [tag] mesh-groups

Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode or interface configuration mode.

N/A

Usage Guide

Configuration The following example displays the mesh groups.

Examples Ruijie# show isis mesh-groups

```
Mesh group (blocked)
FastEthernet 1/1
Mesh group 1 :
FastEthernet 1/0
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.73 show isis neighbors

Use this command to display the IS-IS neighbors..

show isis [tag] neighbors [detail]

Parameter Description	Parameter	Description
	<i>tag</i>	Displays the IS-IS instance.
	<i>detail</i>	Displays the detailed information of all interfaces.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode or interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays details of IS-IS neighbors.

```
Ruijie# show isis neighbors detail

Area (null):
System Id  Type  IP Address    State  Holdtime  Circuit  Interface
r1         L1   1.0.0.2      Up     9         r1.01   GigabitEthernet 0/0
           L2   1.0.0.2      Up     9         r1.01   GigabitEthernet 0/0

Adjacency ID: 1
Uptime: 00:06:25
Area Address(es): 49.1111
SNPA: 00d0.f8bc.de08
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
Level-1 MTID: Standard
Level-2 MTID: Standard
Level-1 Protocols Supported: IPv4, IPv6
Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.74 show isis protocol

Use this command to display relevant protocol information about an IS-IS system.

show isis [tag] protocol

Parameter Description	Parameter	Description
	tag	IS-IS instance.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide N/A

Configuration The following example displays relevant protocol information about an IS-IS system.

Examples

```
Ruijie# show isis protocol
IS-IS Router: (null)
  Binding VRF: vrf
  Mib-Binding: off
  System ID: 0000.0000.0036  IS-type: level-1-2
  Virtual System ID:
    1111.1111.1111, 2222.2222.2222
  Manual area address(es):
    49.0001, 49.0003
  Interfaces supported by IS-IS:
    GigabitEthernet 0/0, GigabitEthernet 0/1
  Redistributing IPv4:
    isis 1, isis 2
  Redistributing IPv6:
    isis 3, isis 4
  Distance: 115
  Generate narrow metrics: Level-1-2
  Accept narrow metrics: Level-1-2
  Generate wide metrics: none
  Accept wide metrics: none
  NSR: enable
  Two-way-maintain: enable
```

Field description:

Field	Description
IS-IS Router	Instance tag
Binding VRF	Name of the VRF bound to the instance
Mib-Binding	Indicates whether the instance is bound with SNMP.
System ID	System ID
IS-type	Level type supported by the instance
Virtual System ID	Extended system ID
Manual area address(es)	Area ID
Interfaces supported by IS-IS	Interface associated with the instance
Redistributing IPv4	Source of redistributed IPv4 routes
Redistributing IPv6	Source of redistributed IPv6 routes
Distance	IS-IS management weight
Generate narrow metrics	Type of the generated narrow metrics

Accept narrow metrics	Type of the accepted narrow metrics
Generate wide metrics	Type of the generated wide metrics
Accept wide metrics	Type of the accepted wide metrics
NSR	Indicates whether the NSR function is enabled for the instance.
Two-way-maintain	Indicates whether the two-way maintenance function is enabled for the instance.

4.75 show isis topology

Use this command to display the topology of the IS-IS router connection.

show isis [*tag*] **topology** [**frr** { **self-originate** | *WORD* | **all** }] [**I1** | **I2** | **level-1** | **level-2**]

Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.
	frr	Displays the IS-IS IP FRR topology.
	<i>WORD</i>	System ID or host name.
	self-originate	Displays the topology of the device.
	all	Displays the topology whose root node is the local device or the IS-IS neighbor.
	I1	Specifies the topology of Level-1.
	level-1	Specifies the topology of Level-1.
	I2	Specifies the topology of Level-2.
	level-2	Specifies the topology of Level-2.

Defaults N/A

Command Mode Privileged EXEC mode/ global configuration mode/ interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays all IS-IS neighbors:

```
Ruijie#show isis topology
Area (null):
IS-IS paths to level-1 routers
System Id    Metric    Next-Hop    SNPA                Interface
r1           10       r1          00d0.f822.33ad     GigabitEthernet 0/0
Ruijie      --
IS-IS paths to level-2 routers
System Id    Metric    Next-Hop    SNPA                Interface
r1           10       r1          00d0.f822.33ad     GigabitEthernet 0/0
```


Ruijie --

The following example displays the topology whose root node is the local device or the IS-IS neighbor.

```
S#show isis topology frr all l1

Area (null):
IS-IS paths to level-1 routers
Self spf topology (S):
System Id      Metric      Next-Hop          SNPA              Role
Interface
S              --
N              8           N                 00e0.2030.00d5    Primary
GigabitEthernet 0/5
E              --           E                 00d0.f822.33d8    Backup
GigabitEthernet 0/6
E              5           E                 00d0.f822.33d8    Primary
GigabitEthernet 0/6
N              --           N                 00e0.2030.00d5    Backup
GigabitEthernet 0/5
D              9           E                 00d0.f822.33d8    Primary
GigabitEthernet 0/6
N              --           N                 00e0.2030.00d5    Backup
GigabitEthernet 0/5

Nbr spf topology (N):
System Id      Metric      Next-Hop          SNPA              Role
Interface
S              8           S                 --               --      --
N              --
E              11          D                 --               --      --
D              7           D                 --               --      --

Nbr spf topology (E):
System Id      Metric      Next-Hop          SNPA              Role
Interface
S              5           S                 --               --      --
N              11          D                 --               --      --
E              --
D              4           D                 --               --      --
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

4.76 show isis virtual-neighbors

Use this command to display the virtual system neighbor information of an IS-IS system.

show isis [tag] virtual-neighbors

Parameter Description	Parameter	Description
	<i>tag</i>	<i>IS-IS instance.</i>

Defaults -

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples

```
Ruijie# show isis virtual-neighbors

Area (null):
Virtual System Id      Type      State
1111.1111.1111        L1        DOWN
                      L2        UP
2222.2222.2222        L1        DOWN
                      L2        UP
```

Field description:

Field	Description
Area	Instance tag
Virtual System Id	Virtual system ID
Type	Neighbor type
State	Neighbor status. UP indicates the level at which the extended LSP fragment is created.

4.77 spf-interval

Use this command to set the minimal interval for the SPF calculation. Use the **no** form of this

command to restore the default minimal interval.

spf-interval [**level-1** | **level-2**] *maximum-interval* [*initial-interval* *hold-interval*]

no spf-interval [**level-1** | **level-2**]

**Parameter
Description**

Parameter	Description
level-1	Applies the configuration only to Level-1.
level-2	Applies the configuration only to Level-2.
<i>maximum-interval</i>	Indicates the maximum interval for performing two consecutive SPF calculations. The value range is 1 to 120 (in seconds). The default value is 10 .
<i>initial-interval</i>	Indicates the waiting time for performing the SPF calculation for the first time. The value range is 0 to 60000 (in milliseconds). The default value is 50 .
<i>hold-interval</i>	Indicates the minimum interval for performing the SPF calculation for the second time. The value range is 10 to 60000 (in milliseconds). The default value is 200 .

Defaults

By default, this command is not configured.

The default SPF interval is 10 seconds, which takes effect at both Level-1 and Level-2.

Command

IS-IS routing process configuration mode

Mode

Usage Guide

Increasing the minimum interval for performing SPF calculations can avoid frequent SPF calculations and waste of CPU resources. However, a larger minimum interval also leads to slower responses to route changes.

The waiting time for performing the SPF calculation for the first time is the initial interval. If the network becomes unstable, the SPF calculation interval is less than the maximum interval, and the interval for performing the SPF calculation for the second time becomes the hold interval. A corresponding penalty is added to this interval: The next interval for the SPF calculation doubles the previous interval for the same SPF calculation, until the SPF calculation interval reaches the maximum interval. Subsequent SPF calculations are performed at the maximum interval. When the network becomes stable, the interval for performing the SPF calculation becomes greater than the maximum interval, and the waiting time for performing the SPF calculation is restored to the initial interval.

Link changes have high requirements for convergence. The initial interval can be set to a small value.

The preceding parameters can also be adjusted to larger values to reduce CPU consumption.

The value of **initial-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of **initial-interval** will be used as the value of **maximum-interval**.

The value of **hold-interval** cannot be greater than that of **maximum-interval**. Otherwise, the value of **hold-interval** will be used as the value of **maximum-interval**.

The value of **initial-interval** cannot be greater than that of **hold-interval**. Otherwise, the value of **initial-interval** will be used as the value of **hold-interval**.

Configuration The following example sets the minimum interval for generating two duplicate SPF packets to 5 seconds, the interval for generating a duplicate SPF packet for the first time to 100 ms, and the interval for generating a duplicate SPF packet for the second time to 200 ms.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# spf-interval 5 100 200
```

The following example sets the minimum interval for generating two duplicate SPF packets to 10 seconds.

```
Ruijie(config)# router isis
Ruijie(config-router)# spf-interval 10
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

4.78 summary-address

Use this command to configure the IPv4 aggregation route. Use the **no** form of this command to delete the aggregation route.

summary-address *ip-address net-mask* [**level-1** | **level-2** | **level-1-2**] [metric *number*]

no summary-address *ip-address net-mask*

Parameter Description

Parameter	Description
<i>ip-address</i>	Indicates the IP address of the summary route.
<i>net-mask</i>	Indicates the subnet mask of the summary route.
level-1	Applies the setting only to Level-1.
level-2	Applies the setting only to Level-2. By default, the setting takes effect for Level-2.
level-1-2	Applies the setting to Level-1 and Level-2.
<i>number</i>	Indicates the metric of the summary route.

Defaults By default, no aggregation route is configured.

Command Mode IS-IS routing process configuration mode

Usage Guide With the aggregation route configured, if there is any reachable address or reachable network segment route in the aggregation route, it will publish the aggregation route instead of the detailed route.

Configuration Ruijie(config)# **router isis**

Examples Ruijie(config-router)# **summary-address 10.10.0.0/24 level-1-2**

Related Commands	Command	Description
	summary-prefix	Configures the IPv6 aggregation route.

Platform N/A

Description

4.79 summary-prefix

Use this command to configure the IPv6 aggregation route. Use the **no** form of this command to delete the aggregation route.

summary-prefix *ipv6-prefix/prefix-length* [**level-1** | **level-2** | **level-1-2**]

no summary-address *ipv6-prefix/prefix-length*

Parameter Description	Parameter	Description
	<i>ipv6-prefix / prefix-length</i>	Aggregation network address and the IP prefix length of the aggregation network address.
	level-1	Applies to the Level-1 only.
	level-2	Applies to the Level-2 only.
	level-1-2	Applies to both Level-1 and Level-2.

Defaults By default, no aggregation route is configured.

Command Address-family ipv6 mode

Mode

Usage Guide With the aggregation route configured, if there is any reachable address or reachable network segment route in the aggregation route, it will publish the aggregation route instead of the detailed route.

Configuration Ruijie(config)# **router isis**

Examples Ruijie(config-router)# **address-family ipv6**

Ruijie (config-router-af)# **summary-prefix 1000::/96 level-1-2**

Related Commands	Command	Description
	summary-address	Configures the IPv4 aggregation route.

Platform N/A

Description

4.80 virtual-system

Use this command to configure an additional system ID for fragment extension. Use the **no** form of this command to remove the additional system ID.

virtual-system *system-id*

no virtual-system *system-id*

Parameter Description	Parameter	Description
	<i>system-id</i>	Additional system ID. The length is 6 bytes.

Defaults No additional system ID is configured by default.

Command IS-IS routing process configuration mode

Mode

Usage Guide Use this command to configure an additional system ID for LSP fragment extension. The system must be enabled with fragment extension mode and configured with the additional system ID to enable LSP fragment extension.

Configuration The following example configures an additional system ID for fragment extension.

Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# virtual-system 0000.0000.0034
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.81 vrf

Use this command to bind the ISIS process with a VRF instance. Use the **no** form of this command to unbind the IS-IS process from the VRF instance.

vrf *vrf-name*

no vrf *vrf-name*

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF instance name. The VRF instance must be configured.

Defaults No IS-IS process is bound with the VRF instance.

Command Mode IS-IS routing process configuration mode

Usage Guide Before you configure this command, the specified VRF instance must be configured. If you want to build the IS-IS v6 neighbor, the multi-protocol VRF and IPv6 protocol must be enabled.

The following restrictions are for binding IS-IS process with VRF instance:

1. The IS-IS process in the same non-default VRF instance must be configured with a different system ID. The IS-IS process in the different VRF instance can be configured with the same system ID.
2. An IS-IS process can be bound with only one VRF instance. A VRF instance can be bound with multiple IS-IS processes.
3. If a VRF instance bound with an IS-IS changes, the IS-IS enabled interfaces which are bound with the VRF instance and the redistribute configuration in IS-IS routing process configuration mode will be removed.

Configuration The following example binds an IS-IS process with a VRF instance.

Examples

```
Ruijie(config)#vrf definition vrf_1
Ruijie(config-vrf)#address-family ipv4
Ruijie(config-vrf-af)#exit-address-family

Ruijie(config)# router isis
Ruijie(config-router)# vrf vrf_1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5 BGP4 Commands

5.1 address-family ipv4

Use this command to enter IPv4 address family configuration mode to configure BGP configuration mode. Use the **no** or **default** form of this command to exit BGP address configuration mode.

address-family ipv4 [unicast|multicast|mdt]

no address-family ipv4 [unicast|multicast|mdt]

default address-family ipv4 [unicast]

	Parameter	Description
Parameter Description	unicast	Optional, detailed IPv4 unicast address prefix
	multicast	Optional, detailed IPv4 multicast address prefix
	mdt	Optional, detailed IPv4 MDT address prefix

Defaults The configuration mode is unicast address prefix by default.

Command

Mode BGP configuration mode

In BGP address configuration mode, use the standard IPv4 address for the configuration.

To return to BGP configuration mode, run the command **exit-address-family**.

Usage

You can enter the multicast mode to configure the BGP of the multicast topology, which is used for RPF detection

Guide

mdt address family mode to configure the BGP of the multicast topology VPN, which is used for ob of the IPv4 multicast routing protocol.

You can enter taining the cross-domain exit agent in the IPv4 multicast routing protocol.

Configuration

The following example enters the IPv4 address family configuration mode.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv4
```

Related

Commands

Command	Description
exit-address-family	Exits the mode.

Platform

Description None

5.2 address-family ipv4 vrf

Use this command to enter the IPv4 VRF address family configuration mode to configure BGP and enable the exchange of route information of a VRF. Use the **no** or **default** form of this command to restore the default setting.

address-family ipv4 vrf vrf-name

no address-family vrf vrf-name

default address-family ipv4 vrf vrf-name

Parameter	Parameter	Description
Description	vrf-name	VRF name

Defaults No vrf is defined by default.

Command

Mode BGP configuration mode

You can execute this command to configure or exit the exchange of route information between PEs and CEs.

**Usage
Guide**

To return to BGP configuration mode, run the **exit-address-family** command.

If IPv4 VRF and IPv6 VRF address family modes of the same VRF are activated at the same time, and the same neighbor is activated in two address family modes, the neighbor's global commands will be displayed in both address family modes at the same time, while its address family commands will be displayed only under respective address family modes.

**Configuration
Examples**

The following example enters the IPv4 VRF address family configuration mode.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv4 vrf vpn1
```

**Related
Commands**

Command	Description
exit-address-family	Exits the configuration mode.

Platform

Description N/A

5.3 address-family ipv6

Use this command to enter IPv6 address family configuration mode and enable the exchange of IPv6 route information. Use the **no** or **default** form of this command to restore the default setting. Use the **exit-address-family** command to exit BGP address-family configuration mode.

address-family ipv6 [unicast]

no address-family ipv6 [unicast]

default address-family ipv6 [unicast]

Parameter	Parameter	Description
Description	unicast	Optional, enters IPv6 unicast address-family configuration mode.

Defaults The configuration mode is unicast address prefix by default.

Command

Mode BGP configuration mode or BGP Scope configuration mode

Usage You can use this command not only to enter IPv6 address-family configuration mode of the BGP to configure the IPv6 neighbors, but also activate neighbors in IPv6 address-family configuration mode after configuring IPv6 neighbors in BGP configuration mode.

Guide

The **exit-address-family** command is used to return to BGP configuration mode.

Configuration

The following example enters the IPv6 address family configuration mode.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv6
```

Related

Commands

Command	Description
exit-address-family	Exits the mode.

Platform

Description None

5.4 address-family ipv6 vrf

Use this command to enter BGP configuration mode, enable the IPv6 route information exchange function under a vrf. Use **no** or **default** form of this command to restore the default setting. Use the **exit-address-family** command to exit BGP address configuration mode.

address-family ipv6 vrf vrf-name

no address-family ipv6 vrf vrf-name

default address-family ipv6 vrf vrf-name

Parameter
Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults No vrf address family is defined by default.

Command

BGP configuration mode

Mode

Usage Guide You can use this command to start configuring (or quit) the exchange of BGP route information between PE or MCE device and CE.

You can use the `exit-address-family` command to return to BGP configuration mode.

- ✔ If ipv4 vrf and ipv6 vrf address family modes of the same vrf are activated at the same time, and same neighbor is activated in two address family modes, the neighbor's global commands will be displayed in both the address family modes at the same time, while its address family commands will only be displayed under respective address family mode.

Configuration The following example enters the IPv6 VRF address family configuration mode.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv6 vrf vpn1
```

Configuration Examples	Command	Description
	<code>exit-address-family</code>	Exits the mode.

Platform N/A

Description

5.5 address-family l2vpn

Use this command to enter the L2VPN address family configuration mode and enable the exchange of L2VPN route information between BGP neighbors. Use the **no** or **default** form of this command to restore the default setting.

address-family l2vpn { vpls | vpws }

no address-family l2vpn { vpls | vpws }

default address-family l2vpn { vpls | vpws }

Parameter Description	Parameter	Description
	vpls	L2VPN VPLS address family.
	vpws	L2VPN VPWS address family.
	evpn	L2VPN EVPN address family.

Defaults No L2VPN address family is defined by default.

Command

Mode BGP configuration mode / BGP scope global configuration mode

Usage

Guide Use the **exit-address-family** command to exit the L2VPN address family configuration mode.

Configuration Examples	<p>The following example enters the L2VPN VPLS address family configuration mode.</p> <pre>Ruijie(config)# router bgp 100 Ruijie(config-router)# address-family l2vpn vpls</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

5.6 address-family vpnv4

Use this command to enter the VPNv4 address family configuration mode and enable the exchange of VPN route information between PE peers. Use the **no** or **default** form of this command to restore the default setting.

address-family vpnv4 [unicast]

no address-family vpnv4 [unicast]

default address-family vpnv4

Parameter	Parameter	Description
Description	unicast	Optional, detailed VPNv4 unicast address prefix.

Defaults No VPNv4 address family is defined by default.

Command

Mode BGP configuration mode / BGP scope global configuration mode

Usage Use the **exit-address-family** command to exit the VPNv4 address family configuration mode.

Guide  The function is only supported by device which supports MPLS L3VPN.

Configuration Examples	<p>The following example enters the VPNv4 address family configuration mode.</p> <pre>Ruijie(config)# router bgp 65000 Ruijie(config-router)# address-family vpnv4</pre>
-------------------------------	--

Related Commands	Command	Description
	exit-address-family	Exits the mode.

Platform

Description N/A

5.7 address-family vpnv6

Use this command to enter the VPNv6 address family configuration mode and enable the exchange of VPN route information between PE peers. Use the **no** or **default** form of this command to restore the default setting.

address-family vpnv6 [unicast]

no address-family vpnv6 [unicast]

default address-family vpnv6

Parameter	Description
unicast	Optional, detailed VPNv6 unicast address prefix. The command without this parameter takes the same effect as the command with this parameter.


Defaults No VPNv6 address family is defined by default.

Command

Mode BGP configuration mode / BGP scope global configuration mode.

Usage Use the **exit-address-family** command to exit the VPNv6 address family configuration mode.

Guide

 The function is only supported by device which supports MPLS L3VPN.

Configuration
Examples

The following example enters the VPNv6 address family configuration mode.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family vpnv6
```

Related
Commands

Command	Description
exit-address-family	Exits the mode.

Platform

Description N/A

5.8 aggregate-address (IPv4)

Use this command to set the aggregate IPv4 route. Use the **no** or **default** form of this command to restore the default setting.

aggregate-address ip-address mask [as-set] [summary-only] [attribute-map map-tag]

no aggregate-address

default aggregate-address ip-address mask

Parameter	Description
<i>ip address</i>	IP address of the aggregate route
<i>mask</i>	Mask of the aggregate route
as-set	Keeps the AS path information of the path in the aggregate address range.
summary-only	Advertises only the aggregate route.
attribute-map	Configures the routing policy to control the route attribute.
<i>map-tag</i>	Route map name. Up to 32 characters is allowed.

Defaults The address aggregation is not configured by default.

Command Mode BGP configuration mode, IPv4 address family configuration mode, or IPv4 VRF address family configuration mode

Usage Guide The BGP-enabled device will advertise all path information both before and after aggregation by default. Use the **aggregate-address summary-only** command to advertise the aggregate route only.

Configuration Examples The following example sets the aggregate IPv4 route.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# aggregate-address 10.0.0.0
255.0.0.0 as-set
```

Command	Description
router bgp	Enables the BGP protocol.

Related Commands

Platform Description None

5.9 aggregate-address (IPv6)

Use this command to set the aggregate IPv6 route. Use the **no** or **default** form of this command to restore the default setting.

aggregate-address ipv6-network / length [as-set] [summary-only] [attribute-map map-tag]

no aggregate-address ipv6-network / length

default aggregate-address ipv6-network/length

Parameter	Description
<i>ipv6-network</i>	IP address prefix of the aggregate route
<i>length</i>	Length of the aggregate route
as-set	Keeps the AS path information of the path in the aggregate address range.

Parameter Description

summary-only	Advertises only the aggregate route.
attribute-map	Configures the routing policy to control the route attribute.
<i>map-tag</i>	Route map name. Up to 32 characters is allowed.

Defaults The address aggregation is not configured by default.

Command Mode BGP IPv6 address-family configuration mode, BGP IPv6 VRF address-family configuration mode or BGP Scope configuration mode.

Usage Guide The BGP-enabled device will advertise all path information both before and after aggregation by default. Use the **aggregate-address summary-only** command to advertise the aggregate route only.

Configuration Examples The following example sets the aggregate IPv6 route.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv6
Ruijie(config-router-af)# aggregate-address 2008::/90 as-set
```

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.

Platform

Description None

5.10 bgp advertise non-transitive extcommunity

Use this command to allow carried non-transitive extcommunity when BGP is notifying EBGp neighbors of a route. Use the **no** or **default** form of this command to restore the default setting.

bgp advertise non-transitive extcommunity

no bgp advertise non-transitive extcommunity


default bgp advertise non-transitive extcommunity

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Non-transitive extcommunity is removed when notifying EBGp neighbors of a route.

Command Mode BGP configuration mode / Scope global configuration mode

Usage Guide By default, when notifying EBGp neighbors of a route, neighbors will not be notified of extcommunity with the "non-transitive" flag. This configuration can enable the notification of non-transitive extcommunity.

-  Non-transitive extcommunity will be carried when notifying alliance EBGP or IBGP neighbors of a route.

Configuration The following example allows carried non-transitive extcommunity.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp advertise non-transitive extcommunity
```

Configuration Examples

Command	Description
<code>router bgp</code>	Enables BGP protocol.

Platform N/A

Description

5.11 bgp always-compare-med

Use this command to compare Multi Exit Discriminator (MED) all the time. Use the **no** or **default** form of this command to restore the default setting.

bgp always-compare-med

no bgp always-compare-med

default bgp always-compare-med

Parameter Description

Parameter	Description
N/A	N/A

Defaults MED of peer paths from the same AS is compared by default.

Command

Mode BGP configuration mode / Scope global configuration mode

Usage Guide

The MED value is compared for paths of peers from the same AS by default. This command can be used to allow comparing MED values for paths from different ASs. If there are multiple valid paths to the same destination, the one with lower MED value has higher priority.

This command is not recommended unless you are sure that different ASs are using the same IGP and routing method.

Configuration Examples

The following example compares Multi Exit Discriminator (MED) all the time.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp always-compare-med
```

Related Commands

Command	Description
<code>show ip bgp</code>	Displays the BGP route entry.

bgp bestpath med confed	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med missing-as-worst	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform**Description** None

5.12 bgp asnotation dot

Use this command to modify the displaying mode of the 4-byte AS notation and the matching type of the regular expression as the dot mode (that is, two dotted decimal numbers). Use the **no** or **default** form of this command to restore the default setting.

bgp asnotation dot**no bgp asnotation dot****default bgp asnotation dot**

Parameter	Parameter	Description
Description	N/A	N/A

Defaults

The 4-byte AS notation is shown in decimal digit, and the regular expression also matches the 4-byte AS notation with decimal digit by default.

Command**Mode** BGP configuration mode / Scope global configuration mode

Our devices support two modes of representing the 4-byte AS notation. One is decimal digit, and the other one is dot mode which represents the 65536 with 1.0. The decimal format is same as the default format, which represents the 4-byte AS notation with decimal digits. The dot mode displays the 4-byte AS notation in the format of ([two high bytes.] two low bytes). If the [two high bytes.] is zero, it will not be displayed. That is, the AS notation represented as 65536 in decimal is 1.0 in the dot mode. In another example, the AS notation is 65534 represented in decimal, while it is represented as 65534 in the dot mode without the zero in front.

Usage**Guide**

No matter which mode will be adopted to display the 4-byte AS notation, both modes can be used when entering the configuration commands. But the representation and displaying mode of the 4-byte AS notation in the regular expression must be the same. Otherwise, the matching will fail. After executing the **bgp asnotation** command, you must use the `clear ip bgp *` to perform the resetting, so as to re-match the filtering condition of the regular expression.



The AS notation is represented as 1 to 65535 no matter using decimal or dot mode.

Configuration The following example modifies the showing mode of the 4-byte AS notation.

Examples

```
Ruijie(config)# router bgp 1.0
Ruijie(config-router)# bgp asnotation dot
```

Related

Commands

Command	Description
show ip bgp summary	Displays the related information of BGP neighbor.

Platform

Description

None

5.13 bgp bestpath as-path ignore

Use this command to disregard the length of the AS path. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

default bgp bestpath as-path ignore

Parameter

Description

Parameter	Description
N/A	N/A

Defaults

The AS path length is considered in choosing the optimal path by default.

Command

Mode

BGP configuration mode / Scope global configuration mode

Usage

Guide

BGP will not take the length of the AS path into account when it selects the optimal path as specified in RFC1771. In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path into account when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.

Configuration

Examples

The following example disregard the length of the AS path.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath as-path ignore
```

Related

Commands

Command	Description
show ip bgp	Displays the BGP route entry.

Platform

Description

None

5.14 bgp bestpath as-path multipath-relax

Use this command to enable AS path multipath-relax (only comparing the AS path length) for BGP multipathing load. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath as-path multipath-relax
no bgp bestpath as-path multipath-relax
default bgp bestpath as-path multipath-relax

Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	BGP requires that AS path attributes must be the same when calculating equal-cost multipath (ECMP) by default.	
Defaults	BGP configuration mode / Scope global configuration mode	
Usage Guide	BGP compares AS path attributes in a precise way when selecting the optimal path as ECMP by default. Only paths with same AS path attributes can constitute equal-cost paths. As a result, BGP multipathing load balancing cannot be implemented in an application scenario. After AS path multipath-relax is enabled, only the AS path length is compared, allowing the implementation of BGP multipathing load balancing.	
Configuration Examples	The following example enables AS path multipath-relax for BGP multipathing load.	
	<pre>Ruijie(config)# router bgp 65530 Ruijie(config-router)# bgp bestpath as-path multipath-relax</pre>	
Related Commands	Command	Description
	router bgp	Enables BGP.
	show ip bgp	Displays BGP routing entries.
Platform Description	None	

5.15 bgp bestpath compare-confed-aspash

Use this command to compare the AS path length of the confederation from the same external routes when selecting the optimal path, with smaller AS path in the confederation for higher path priority. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath compare-confed-aspash
no bgp bestpath compare-confed-aspash

default bgp bestpath compare-confed-aspath

Parameter	Parameter	Description
Description	N/A	N/A

Defaults

The AS path of the EBGP peer routes inside the same confederation is not compared by default when selecting the optimal path. Instead, the routing method is implemented.

Command**Mode**

BGP configuration mode / Scope global configuration mode

Usage**Guide**

During the selection of the same routing information from the peer of the internal EBGP By default, the AS path of the confederation is not compared. This command is used to compare the AS path of the confederation.

Note that if a route contain no AS path of the confederation, it is impossible to implement the AS path comparison for that route.

Configuration**Examples**

The following example compares the AS path length of the confederation.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath compare-confed-aspath
```

Related**Commands**

Command	Description
show ip bgp	Displays the BGP route entry.
bgp router-id	Sets the BGP Device ID.

Platform**Description**

None

5.16 bgp bestpath compare-routerid

Use this command to compare the router ID of the same external routes when selecting the optimal path, with smaller router ID for higher path priority. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

default bgp bestpath compare-routerid

Parameter	Parameter	Description
Description	N/A	N/A

Defaults

If two paths received from different EBGP peers have the same path, the first one is considered with higher priority by default.

Command**Mode** BGP configuration mode / Scope global configuration mode**Usage**

If two paths with identical path attributes are received from different EBGP peers during the selection of the optimal path, we will select the optimal path according to the sequence of receiving the paths by default. You can select the path with smaller Device ID as the optimal path by configuring the following commands.

Configuration

The following example compares the router ID of the same external routes.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath compare-routerid
```

Related**Commands**

Command	Description
show ip bgp	Displays the BGP route entry.
bgp router-id	Sets the BGP Device ID.

Platform**Description** None

5.17 bgp bestpath med confed

Use this command to compare the MED value of the path of the internal peer from AS confederation during selecting the optimal path. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath med confed [missing-as-worst]

no bgp bestpath med confed [missing-as-worst]

default bgp bestpath med confed [missing-as-worst]

Parameter**Description**

Parameter	Description
missing-as-worst	Sets the priority of the path without MED attribute as the lowest.

Defaults

The MED value of the path of the peer inside the AS confederation is not compared by default when selecting the optimal path.

Command**Mode** BGP configuration mode / Scope global configuration mode**Usage**

The MED attribute of the path is transferred between the ASs inside the confederation. You may set always comparing this value.

Guide**Configuration**

The following example compares the MED value of the path of the internal peer.

Examples

```
Ruijie(config)# router bgp 65000
```

```
Ruijie(config-router)# bgp bestpath med confed
```

**Related
Commands**

Command	Description
show ip bgp	Displays the BGP route entry.
bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med missing-as-worst	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform

Description None

5.18 bgp bestpath med missing-as-worst

Use this command to set the priority of the path without MED attribute as the lowest when selecting the optimal path. Use the **no** or **default** form of this command to restore the default setting.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

default bgp bestpath med missing-as-worst

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

If a path without MED attribute is received, the MED value of the path is 0 by default. Such route has the highest priority according to the above-mentioned rule.

Command

Mode BGP configuration mode / Scope global configuration mode

**Usage
Guide**

The MED value of a path without MED attribute will be 0 by default. For the smaller the MED value, the higher the priority of the path is, the MED value of this path has the highest priority. This command can be used to figure the path without MED attribute has the lowest priority.

**Configuration
Examples**

The following example sets the priority of the path without MED attribute as the lowest.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath medmissing-as-worst
```

**Related
Commands**

Command	Description
show ip bgp	Displays the BGP route entry.

bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med confed	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform**Description** None

5.19 bgp client-to-client reflection

Use this command to enable the route reflection function between clients on the device. Use the **no** or **default** form of this command disables the route reflection function between clients.

bgp client-to-client reflection

no bgp client-to-client reflection

default bgp client-to-client reflection

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled without the client for route reflection by default.

Command

Mode BGP configuration mode / Scope global configuration mode

Usage Guide

In general, it is unnecessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the route among clients. However, if the full connection relationship is established for all clients, the function for the route reflector to reflect the client route can be disabled.

To disable the route reflection function, use the command **no bgp client-to-client reflection**.

Configuration Examples

The following example shows how to enable the route reflection function between clients on the device.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# no bgp client-to-client
reflection
```

Related Commands

Command	Description
bgp cluster-id	Configures the cluster ID of the route reflector.
neighbor route-reflector-client	Configures the client of the route reflector and configure itself as the route reflector.

Platform	
Description	None

5.20 bgp cluster-id

Use this command to configure the cluster ID of the route reflector. Use the **no** or **default** form of this command to restore it to the default setting.

bgp cluster-id *cluster-id*

no bgp cluster-id

default bgp cluster-id

Parameter	Description
Description	<i>cluster-id</i>
	Cluster ID of the route reflector, an IP address of up to four bytes or an integer (must be entered in form of IP address)

Defaults The cluster id is the router-id of the route reflector by default.

Command

Mode BGP configuration mode / Scope global configuration mode

Usage

In general, one group is only configured with one route reflector. In this case, the Device ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.

Guide

Configuration

The following example configures the cluster ID of the route reflector.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp cluster-id 10.0.0.1
```

Related Commands	Command	Description
	bgp client-to-client reflection	Configures the route reflection between clients.
	neighbor route-reflector-client	Configures the client of the route reflector and configures itself as the route reflector.

Platform	
Description	None

5.21 bgp confederation identifier

Use this command to configure the AS confederation identifier. Use the **no** or **default** form of this command to restore the default setting.

bgp confederation identifier *as-number*

no bgp confederation identifier

default bgp confederation identifier

**Parameter
Description**

Parameter	Description
<i>as-number</i>	AS confederation identifier in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, which is represented as 1 to 65535.65535 in dot mode.

Defaults There is no confederation identifier by default

Command

Mode BGP configuration mode or BGP Scope Global configuration mode

**Usage
Guide**

The confederation is a measure to reduce the connections of IBGP peers within the AS. One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.

Configuration The following example configures the AS confederation identifier.

Examples

```
Ruijie(config-router)# bgp confederation identifier 65000
```

**Related
Commands**

Command	Description
bgp confederation peers	Adds member AS of the AS confederation.

Platform

Description None

5.22 bgp confederation peers

Use this command to configure member ASs of the AS confederation. Use the **no** or **default** form of this command to restore the default setting.

bgp confederation peers *as-number* [...*as-number*]

no bgp confederation peers *as-number* [...*as-number*]

default bgp confederation peers [*as-number* [...*as-number*]]**Parameter
Description**

Parameter	Description
<i>as-number</i>	Member ASs in the confederation range from 1 to 65535. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.

Defaults

There is no confederation member by default.


Command**Mode**

BGP configuration mode or BGP Scope Global configuration mode

**Usage
Guide**

The confederation is a measure to reduce the connections of BGP peers within the AS. One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. The whole external confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.

This command is used to specify the member AS of a confederation.

 This command can configure up to 15 members of a confederation at one time. For more members, enter them for several times.

Configuration

The following example configures member ASs of the AS confederation.

Examples

```
Ruijie(config-router)# bgp confederation peers 65000 65100
```

**Related
Commands**

Command	Description
bgp confederation identifier	Configures the confederation identifier.

Platform**Description**

None

5.23 bgp dampening

Use this command to enable the routing attenuation and set the attenuation parameters in the address-family or routing configuration mode. Use the **no** or **default** form of this command to restore the default setting.

bgp dampening [*half-life* [*reusing suppressing duration*] | *route-map name*]

no bgp dampening

default bgp dampening

Parameter	Description
<i>half-life</i>	Half-life period, ranging from 1 to 45 minutes
<i>reusing</i>	When the penalty value reaches this value, the routing suppression is cancelled. The value ranges from 1 to 10,000.
<i>suppressing</i>	When the penalty value reaches this value, routing is suspended. The value ranges from 1 to 20000.
<i>duration</i>	Maximum time for routing suppression, ranging from 1 to 255 minutes
<i>name</i>	Route-map name, apply the routing attenuation to the specified route through the route-map.

**Parameter
Description****Defaults**

This function is disabled by default.

**Command
Mode**

BGP configuration mode, BGP IPv4 unicast address-family configuration mode, BGP IPv4 multicast address-family configuration mode, BGP IPv4 MDT address-family configuration mode, BGP IPv4 VRF address-family configuration mode, BGP IPv6 unicast address-family configuration mode, BGP IPv6 unicast address-family configuration mode, or BGP IPv6 multicast address-family configuration mode.

**Usage
Guide**

The **bgp dampening** command is used to suppress unstable BGP routing. The BGP uses the penalty value to describe routing suppression intensity. The penalty value increases 1000 when the routing oscillation is performed once. The suppressed routes will not be used during the BGP routing election.

The **bgp dampening** command is used to suppress unstable EBGP routes and does not take effect to IBGP routes.

The BGP uses the penalty value to describe the route stability. A larger penalty value indicates a more unstable route. The penalty value increases by 1000 when route oscillation occurs (upon receiving withdraw packets). The penalty value does not increase when the upper limit is reached. The upper limit is determined based on the configured duration value and calculated using the following formula: $\text{Penalty upper limit} = 2^{(\text{Duration}/\text{Half-life})} \times \text{Reusing}$. In addition, the penalty upper limit cannot be greater than 20000. Therefore, the duration, half-life, and reusing values need to be adjusted based on the network conditions. The relationship among these parameters are as follows:

$\text{Half-life} \leq \text{Duration}$

$\text{Reusing} \leq \text{Suppressing} \leq \text{Penalty upper limit}$

You can also specify only the half-life value. In this case, the duration value is (half-life x 4), the reusing value is 750, and the suppressing value is 2000.

EBGP routes whose penalty value exceeds the suppressing value will be suppressed. Suppressed routes will not be used during BGP route election and will not be advertised to other BGP peers. If route oscillation occurs in suppressed routes, the penalty value will continue to increase until the penalty upper limit is reached.

The penalty value of suppressed routes will decrease by a half each time the half-life time passes. When the penalty value decreases to the reusing value, routes whose attribute is update in the last update will participate in BGP route election again. When the penalty value decreases to 0, routes

whose attribute is withdraw in the last update will be deleted from the BGP route table.

Configuration The following example enables the routing attenuation and set the attenuation parameters.

Examples Ruijie(config-router)# bgp dampening 30 1500 10000 120

	Command	Description
Related Commands	clear ip bgp dampening	Clears the BGP suppression and cancels the suppression for the routes.
	show ip bgp dampening dampened-paths	Displays the suppressed route information.

Platform

Description None

5.24 bgp default ipv4-unicast

Use this command to set the IPv4 unicast address as the default address family. Use the **no** or **default** form of this command to restore the default setting.

bgp default ipv4-unicast

no bgp default ipv4-unicast

default bgp default ipv4-unicast

	Parameter	Description
Parameter Description	N/A	N/A

Defaults The IPv4 unicast address is the default address family.

Command

Mode BGP configuration mode or BGP Scope Global configuration mode

Usage

Guide This command is used to set the default address family of BGP as the IPv4 unicast address.

Configuration The following example sets the IPv4 unicast address as the default address family.

Examples Ruijie(config-router)# default ipv4-unicast

	Command	Description
Related Commands	address-family ipv4	Enters the IPv4 address mode.

Platform

Description None

5.25 bgp default local-preference

Use this command to set the default local-preference attribute value. Use the **no** or **default** form of this command to restore the default setting.

bgp default local-preference *value*

no bgp default local-preference

default bgp default local-preference

Parameter	Parameter	Description
Description	<i>value</i>	Local priority attribute, in the range from 0 to 4294967295

Defaults The local preference value is 100 by default.

Command

Mode BGP configuration mode or BGP Scope configuration mode.

Usage The BGP takes the local preference as the foundation to compare with the priority of the path learned from IBGP peers. The larger the local preference value, the higher the priority of the path is.

Guide The BGP speaker sends the external route received to the IBGP peers to add the local priority value.

Configuration The following example sets the default local-preference attribute value.

Examples

```
Ruijie(config-router)# bgp default local-preference 200
```

Command	Description
show ip bgp	Displays the BGP route entry.
bgp always-compare-med	Allows comparing the MED value of the path of the peer from different ASs when electing the optimal path.
bgp bestpath med confed	Allows comparing the MED value of paths of internal peers from AS community when electing the optimal path.
bgp bestpath med missing-as-worst	Allows setting the priority of the path without MED attribute as the lowest when electing the optimal path.

Platform

Description None

5.26 bgp default route-target filter

Use this command to enable the route-target filtering. For the VPNV4 routes, filter the community attributes of the route-target by default. Use the **no** or **default** form of this command to disable this function.

bgp default route-target filter

no bgp default route-target filter

default bgp default route-target filter

Parameter
Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command
Mode

BGP configuration mode, VPNv4 address-family configuration mode, or BGP L2VPN VPLS/VPWS address-family configuration mode.

Usage
Guide

After receiving the VPNv4 route, use the community attributes list of the route-target to filter and distribute different VRFs. With the no form of this command used, the BGP will receive all VPNv4 routes no matter whether these filtered VPNv4 routes will be received by route-target of local VRF. With the PE route-reflector-client configured for the BGP, the VPNv4 route will not be processed through the route-target filtering. In this case, whether the BGP is enabled, the actions are the same without the route-target filtering.

 The function is only supported by device which supports BGP MPLS/VPN.

Configuration
Examples

The following example enables the route-target filtering.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# no bgp default route-target filter
```

Related
Commands

Command	Description
neighbor route-reflector-client	Configures the route-reflector-client, and sets itself as the route reflector.

Platform
Description

N/A

5.27 bgp deterministic-med

Use this command to set comparing preferentially the MED values of peer paths from the same AS. By default, the comparison is based on the received order, and the one received the last is compared first. Use the **no** or **default** form of this command to restore the default setting.

bgp deterministic med

no bgp deterministic med

default bgp deterministic-med

Parameter

Parameter	Description
-----------	-------------

Description	N/A	N/A
--------------------	-----	-----

Defaults This function is disabled by default.

Command

Mode BGP configuration mode or BGP Scope Global configuration mode

Usage Guide They will be compared with each other according to the sequence the paths are received when the optimal path is selected by default. Execute the following operations in the BGP configuration mode to compare paths of peers from the same AS firstly:

Configuration Examples The following example sets the comparing preferentially MED values.

```
Ruijie(config-router)# bgp deterministic med
```

Related

Commands

Command	Description
show ip bgp	Displays the BGP route entry.
bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med confed	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp bestpath med missing-as-worst	Compares paths of peers from the same AS when selecting the optimal path.

Platform

Description None

5.28 bgp enforce-first-as

Use this command to reject the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number. Use the **no** or **default** form of this command to disable this function.

bgp enforce-first-as

no bgp enforce-first-as

default bgp enforce-first-as

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command

Mode BGP configuration mode or BGP Scope Global configuration mode

Usage The AS number of the device is put into the path section by default to update the update message.

Guide**Configuration**

The following example rejects the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number.

Examples

```
Ruijie(config-router)# bgp enforce-first-as
```

Related**Commands**

Command	Description
show ip bgp	Displays the BGP route entry.

Platform**Description**

None

5.29 bgp fast-external-fallover

When the network interface used in establishing the connection of the directly-connected EBGP peer fails, use this command to establish the BGP session connection quickly. Use the **no** or **default** form of this command to disable this function.

bgp fast-external-fallover

no bgp fast-external-fallover

default bgp fast-external-fallover

Parameter**Description**

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command**Mode**

BGP configuration mode or BGP Scope Global configuration mode

Usage**Guide**

This command takes effect only for the directly-connected EBGP neighbor.

Configuration

The following example creates the fast BGP session.

Examples

```
Ruijie(config-router)# bgp faster-external-fallover
```

Related**Commands**

Command	Description
router bgp	Enables the BGP protocol.

Platform**Description**

None

5.30 bgp fast-reroute

Use this command to enable BGP Fast Reroute. Use the **no** or **default** form of this command to restore the default setting.

bgp fast-reroute

no bgp fast-reroute





default bgp fast-reroute

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP configuration mode/ BGP IPv4 unicast address family configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP scope global configuration mode.

Usage Guide

-  The BGP Fast Reroute function is supported in the BGP IPv4 unicast address family configuration mode and the BGP IPv4 VRF address family configuration mode.
-  Only one backup route will be generated and the next-hop of this backup route cannot be the same as that of the preferred route.
-  When ECMP is enabled, the FRR cannot generate backup route.
-  When this function is enabled in the BGP IPv4 VRF address family configuration mode, the priority of BGP FRR is lower than that of VPN FRR. So when the VPN FRR is enabled in IPv4 VRF configuration mode, BGP FRR does not take effect unless VPN FRR is unable to calculate the backup route.

Configuration Examples

The following example enables BGP Fast Reroute.

```
Ruijie(config)# router bgp 65530
Ruijie(config-router)# bgp faster-reroute
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

N/A

5.31 bgp graceful-restart

Use this command to enable the global BGP graceful restart function. Use the **no** or **default** form of this command to disable BGP graceful restart.

bgp graceful-restart

no bgp graceful-restart

default bgp graceful-restart

Parameter	Parameter	Description
Description	N/A	N/A

Defaults By default, BGP graceful restart is enabled so as to help neighbors to perform graceful restart.


Command

Mode BGP configuration mode or BGP Scope Global configuration mode

The ability of the BGP is advertised and negotiated through the ability field of the Open message. The ability is negotiated during initially setting up the connection. So both sides must reach the consistency of the ability. If it is not supported by any side, this router device will perform the GR incorrectly.

With the GR function enabled, the connected Open message will carry the GR ability field to perform the negotiation of the GR ability. To implement the GR correctly, the GR function must be enabled on both sides of the neighbors.

Usage Guide

 This command does not take effect immediately on all BGP connections that are set up successfully. To negotiate the GR ability immediately, you need to restart the BGP connection to make the local device negotiate the GR ability with the Peer again by using the clear ip bgp command.

The BGP graceful-restart is used to forward data continuously of the whole network, it requires the device to keep the BGP routing entry valid and forward data continuously when restarting the BGP protocol. Supporting the continuous forwarding during the restarting is related to the hardware ability.

Configuration Examples

The following example enables the graceful restart function of the global BGP.

```
Ruijie(config)# router bgp 500
Ruijie(config-router)# bgp graceful-restart
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
bgp graceful-restart restart-time	Configures the restart time of the BGP graceful-restart.

Platform

Description N/A

5.32 bgp graceful-restart disable

Use this command to disable GR capability of a BGP address family. Use the **no** or **default** form of this command to restore the default setting.

bgp graceful-restart disable

no bgp graceful-restart disable

default bgp graceful-restart disable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The function is enabled by default.

Command Mode BGP configuration mode, IPv4 unicast address family mode, VPNv4 address family mode, IPv4 tag address family mode and IPv6 unicast address family mode

Usage Guide When BGP GR function is enabled, the GR capability for all address families is enabled by default, except for address families that do not support GR capability. After GR capability is enabled, you can use this command in the address family mode to disable the address family's GR capability. The Configuration of this command in BGP mode is effective on IPv4 Unicast address family. When BGP GP function is disabled, GR capability is disabled for all address families.

Configuration Examples The following example disables the graceful restart function of the BGP IPv4 address family.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp graceful-restart
Ruijie(config-router)# address-family ipv4
Ruijie(config-router-af)# bgp graceful-restart disable
```

Configuration Examples	Command	Description
	bgp graceful-restart	Enables BGP's GR capability.
	address-family ipv4	Enters BGP IPv4 address family mode.

Platform Description N/A

5.33 bgp graceful-restart restart-time

Use this command to configure the restart time of the BGP graceful-restart. Use the **no** or **default** form of this command to restore the default setting.

bgp graceful-restart restart-time *restart-time*

no bgp graceful-restart restart-time

default bgp graceful-restart restart-time

Parameter	Description
<i>restart-time</i>	GR Restarter-hoped longest waiting time before re-establishing the connection between the GR Helper and the GR Restarter, in the range from 1 to 3600 in the unit of seconds.

Parameter
Description

Defaults The default is 120.


Command

Mode BGP configuration mode or BGP Scope Global configuration mode.

The restart time is advertised by GR Restarter to GR Helper, it is GR Restarter-hoped longest waiting time before re-establishing the connection between GR Helper and GR Restarter. After this time, if the BGP connection with GR Restarter is not in Established status, GR Helper will consider this BGP session failed and will restore the normal BGP. All the routing of the neighbor will be deleted during this period, affecting the data redistribution.

The restart time is advertised in the GR ability field of the BGP Open message. The GR restart time of the two ends of the session is not required to be the same, but it is recommended.

Usage Guide

 This command does not take effect immediately on all BGP connections that are set up successfully. To advertise the newly set restart time to the GR helper, you need to restart the BGP connection to negotiate the GR ability again and advertise the restart time by using the `clear ip bgp` command. The configured restart time should not be greater than the Hold Time of the BGP peer, if so, the Hold time will be the restart time when the GR ability is advertised to the BGP peer.

The following example configures the restart time of the BGP graceful-restart.

```
Ruijie(config)# router bgp 500
Ruijie(config-router)# bgp graceful-restart
Ruijie(config-router)# bgp graceful-restart restart-time 150
Ruijie(config-router)# no bgp graceful-restart restart-time
```

Configuration Examples

Related
Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform N/A
Description

5.34 bgp graceful-restart stalepath-time

Use this command to configure the time to help the device keep the route valid when executing the BGP graceful-restart. Use the **no** or **default** form of this command to restore the default setting.

bgp graceful-restart stalepath-time stalepath-time *time*

no bgp graceful-restart stalepath-time

default bgp graceful-restart stalepath-time

Parameter	Description
<i>time</i>	Longest time used to keep the stale route valid after restoring the connection with the neighbors, in the range from 1 to 3600 in the unit of seconds

Defaults The default is 360.

Command

Mode BGP configuration mode

**Usage
Guide**

This command is configured for the parameters of the GR Helper. The stalepath-time is the longest time of the GR Helper waiting to receive the EOR mark of the Restarter after restoring the connection with the GR Restarter. When the GR Helper detects that the connection with the GR Restarter fails, the original route of the Restarter is marked as the "Stale". However these routes are still used for the routing calculation and forwarding.

The GR Helper updates the routes and cancels the "Stale" mark according to route updating information received from the GR Restarter. If routes marked as "Stale" are not updated in the stalepath-time period, they will be deleted. This mechanism is used to avoid failure in convergence of routes when the GR Helper fails to receive the EOR mark of the GR Restarter for a long time.

**Configuration
Examples**

The following example configures the restart time of the BGP graceful-restart.

```
Ruijie(config)# router bgp 500
Ruijie(config-router)# bgp graceful-restart
Ruijie(config-router)# bgp graceful-restart stalepath-time 240
```

**Related
Commands**

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

**Platform
Description** N/A

5.35 bgp initial-advertise-delay

Use this command to configure the delay period before a BGP device sends its initial updates to peers. Use the **no** form or **default** form of this command to restore the default setting.

bgp initial-advertise-delay *delay-time* [*startup-time*] [**wait-for-controller]**

no bgp initial-advertise-delay

default bgp initial-advertise-delay

Use this command to enable the BGP delayed advertisement upon system restart. Thus, the route will be immediately sent after the prefix-list policy is matched. Use the **no** form or **default** form of this command to restore the default setting.

bgp initial-advertise-delay prefix-list *prefix-list-name*

no bgp initial-advertise-delay prefix-list

default bgp initial-advertise-delay prefix-list

Parameter
Description

Parameter	Description
<i>delay-time</i>	The delay period, in seconds, before a BGP device sends its updates. The range is from 1 to 600. The default value is 1 second.
<i>startup-time</i>	The time for the BGP device restart. In the period, the neighbor does not send its updates to peers. The range is from 5 to 584,000. The unit is second and the default value is 600 seconds.
<i>prefix-list-name</i>	Name of the prefix-list. It cannot exceed 32 characters.
wait-for-controller	Configures the wait-for-controller command to ensure that routes are advertised only after the controller delivers configuration messages and receives EOR messages from the neighbors.

Defaults

The initial advertisement delay is disabled by default.

Command**Mode**

BGP configuration mode

This command is used to configure parameters for delayed neighbor route advertisement during device restart.

delay-time indicates the longest time for sending a route to a neighbor after the BGP neighbor relationship is established. In normal cases, after the neighbor relationship is established, the first route is advertised immediately and subsequent routes are advertised based on the default time. For details, see the **neighbor advertisement-interval** command. **startup-time** indicates the configurable startup time and starts to count when the configuration command takes effect. Within the time specified by **startup-time**, routes to BGP neighbors are advertised periodically based on **delay-time**. This command can be used to change the route advertisement behavior from the BGP peer to neighbors after device restart. The **wait-for-controller** command is used to wait for route advertisement messages from the controller and trigger the BGP route advertisement behavior after EOR messages are received from neighbors. If EOR messages are not received from neighbors within the time specified by **startup-time**, routes are sent forcibly.

Usage**Guide**

The prefix-list policy is configured to ensure that partial routes can be normally delivered. The prefix-list policy applies to distributed routes. Matched routes will be normally delivered without being affected by delayed advertisement. For details about the address family scope to which the prefix-list policy applies, see the **neighbor prefix-list** command.

This command is used by the administrator to adjust the BGP route advertisement behavior during device restart based on the hardware conditions, number of neighbors, number of routes, and actual deployment requirements.

The following example configures initial delay to 60 seconds within 500 seconds after BGP restart.

Configuration**Examples**

```
Ruijie(config)# router bgp 500
Ruijie(config-router)# bgp initial-advertise-delay 60 500
```

Related**Commands**

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform

N/A

Description

5.36 bgp log-neighbor-changes

Use this command to log the BGP status changes without turning on debug. Use the **no** or **default** form of this command to disable this function.

bgp log-neighbor-changes

no bgp log-neighbor-changes

default bgp log-neighbor-changes

Parameter**Description**

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command**Mode**

BGP configuration mode or BGP Scope Global configuration mode

Usage

The debug command can also be used to log BGP status changes. But this command may consume many resources.

Guide**Configuration**

The following example logs the BGP status changes without turning on debug.

Examples

```
Ruijie(config-router)# bgp log-neighbor-changes
```

Related**Commands**

Command	Description
router bgp	Enables the BGP protocol.

Platform**Description**

None

5.37 bgp maxas-limit

Use this command to set the maximum number of ASs in the BGP AS-PATH attribute. Use the **no** or **default** form of the command to restore the default configuration.

bgp maxas-limit *number*

no bgp maxas-limit

default bgp maxas-limit

Parameter	Description
<i>number</i>	The maximum number of ASs in the BGP AS-PATH attribute. The range is from 1 to 512.

Defaults No maximum number of ASs is set by default.

Command

Mode BGP configuration mode/ BGP scope global configuration mode.

Usage The routes exceeding the AS number limit are discarded directly, After changing the configuration, use the **clear** command to reset the neighbor and make the configuration take effect.

Configuration The following example sets the maximum number of ASs in the BGP AS-PATH attribute to 100.

Examples

```
Ruijie(config-router)# bgp maxas-limit 100
```

Related	Command	Description
Commands	N/A	N/A

Platform

Description N/A

5.38 bgp mp-error-handle session-retain

Use this command to retain BGP sessions when BGP protocol detects errors in multi-protocol route attributes. Use the **no** or **default** form of this command to restore the default setting.

bgp mp-error-handle session-retain [**refresh-timer** *time*]

no bgp mp-error-handle session-retain

default bgp mp-error-handle session-retain

Parameter	Description
refresh-timer <i>time</i>	Configures the waiting time for auto route recovery. The parameter ranges from 10 to 4294967296 in the unit of seconds. The default is 120.

Defaults By default, BGP sessions will be interrupted when multi-protocol attribute errors are detected.

Command Mode BGP configuration mode or BGP Scope Global configuration mode

Usage Guide By default, when UPDATA packets are received from a neighbor, BGP sessions will be interrupted if multi-protocol attribute errors are detected, which will cause oscillation of routes of all the address families of the neighbor. An address family's route error will affect the stability of routes of other address families. After this command is configured, when an error of the route attribute of an address family occurs, all the route information of the address family and neighbor will be deleted, thus preventing impact on the BGP session and other protocol address families, improving BGP protocol's stability.

The option `recovery-time` is used to configure the waiting time for auto route recovery. To use the option, the neighbor must support the route refreshing capability. After `recovery-time` expires, BGP will send a route-refresh message to the neighbor's address family and re-notify the neighbor of the address family's all route information.

Configuration Examples The following example retains BGP sessions when BGP protocol detects errors in multi-protocol route attributes.

```
Ruijie(config-router)# bgp mp-error-handle session-retain
```

Configuration Examples	Command	Description
	N/A	N/A

Platform Description N/A

5.39 bgp nexthop trigger delay

Use this command to configure the delay time for updating the routing table when the nexthop of the BGP route changes. Use the **no** or **default** form of this command to restore the default setting.

bgp nexthop trigger delay *delay-time*

no bgp nexthop trigger delay

default bgp nexthop trigger delay

Parameter Description	Parameter	Description
	<i>delay-time</i>	Delay time for updating the routing table when the nexthop changes, in the range from 0 to 100 in the unit of seconds

Defaults The default is 5.

Command BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP

Mode	IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.
Usage	This command is used to configure the delay time for updating the routing table when the nexthop changes, it takes effect when the bgp nexthop trigger enable switch is opened.
Guide	

Configuration Examples	The following example retains BGP sessions when BGP protocol detects errors in multi-protocol route attributes.
	<pre>Ruijie(config-router)# bgp nexthop trigger delay 30</pre>

Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>bgp nexthop trigger enable</td> <td>Enables the nexthop trigger.</td> </tr> </tbody> </table>	Command	Description	bgp nexthop trigger enable	Enables the nexthop trigger.
Command	Description				
bgp nexthop trigger enable	Enables the nexthop trigger.				

Platform	
Description	None

5.40 bgp nexthop trigger enable

Use this command to enable the nexthop trigger update function. Use the **no** or **default** form of this command to disable this function.

bgp nexthop trigger enable

no bgp nexthop trigger enable

default bgp nexthop trigger enable

Parameter	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
Description					

Defaults This function is enabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address-family configuration mode, BGP IPv4/IPv6 VRF address-family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address-family configuration mode or BGP Scope configuration mode.

Usage

Guide This command is used to enable the nexthop trigger update function.

Configuration Examples	The following example enables the nexthop trigger update function.
	<pre>Ruijie(config-router)# bgp nexthop trigger enable</pre>

Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Bgp nexthop trigger delay</td> <td>Sets the delay time for updating the routing table when the nexthop changes.</td> </tr> </tbody> </table>	Command	Description	Bgp nexthop trigger delay	Sets the delay time for updating the routing table when the nexthop changes.
Command	Description				
Bgp nexthop trigger delay	Sets the delay time for updating the routing table when the nexthop changes.				

Platform	
Description	None

5.41 bgp notify unsupported-capability

Use this command to enable the neighbor address family capability detection function. Use the **no** or **default** form of this command to restore the default setting.

bgp notify unsupported-capability

no bgp notify unsupported-capability

default bgp notify unsupported-capability

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP configuration mode or BGP Scope Global configuration mode

Usage Guide When BGP neighbor address family capability negotiation is not fully consistent, neighbors can still be connected. After this command is configured, when an address family capability supported by the local device is not supported by the neighbor device, Notification packet that carries the address family that does not support the capability will be send.

Configuration Examples The following example enables the neighbor address family capability detection function.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp notify unsupported-capability
```

Configuration Examples	Command	Description
	router bgp	Enables BGP protocol.

Platform	N/A
Description	

5.42 bgp redistribute-internal

Use this command to control BGP whether to allow redistributing routes learned from IBGP, such as RIP, OSPF and ISIS, to the IGP protocol. Use the **no** or **default** form of this command to disable this function.

bgp redistribute-internal

no bgp redistribute-internal**default bgp redistribute-internal**

	Parameter	Description
Parameter		
Description	N/A	N/A

Defaults IBGP routes are allowed by default to be redistributed to the IGP protocol.

Command Mode BGP configuration mode, IPv4/IPv6 Unicast address family configuration mode, IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide This command is used to control whether IBGP routes are allowed to be redistributed to the IGP protocol.

Configuration Examples The following example enables the BGP to learn the redistributing routes from IBGP.

```
Ruijie(config-router)# bgp redistribute-internal
```

	Command	Description
Related Commands	redistribute	Redistributes routes learned from other protocols.

Platform Description None

5.43 bgp router-id

Use this command to configure the ID-IP address of the device. Use the **no** or **default** form of this command to restore the default setting.

bgp router-id ip-address**no bgp router-id****default bgp router-id**

	Parameter	Description
Parameter		
Description	<i>ip address</i>	IP address

Defaults The loop-back interface of the device is selected preferentially by default. If it does not exist, the device route-id of the device is used.

Command Mode BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope Global configuration mode.

Usage Guide This command is used to configure IP address, the ID of the device when running the BGP protocol.

Configuration The following example configures the ID-IP address of the device.

Examples Ruijie(config-router)# bgp router-id 10.0.0.1

	Command	Description
Related Commands	show ip bgp dampening dampened-paths	Displays the suppressed routing information.
	bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform

Description None

5.44 bgp scan-rib disable

Use this command to update the routing table by event triggering. Use the **no** or **default** form of this command to restore the default setting.

bgp scan-rib disable

no bgp scan-rib disable

default bgp scan-rib disable

	Parameter	Description
Parameter Description	N/A	N/A

Defaults Timely scan and update is enabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address-family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode and BGP Scope configuration mode.

Usage Guide BGP provides two route update mechanisms: regular-scanning update and event-triggering update. Regular-scanning update indicates that BGP uses an internal timer to start scanning regularly and update the routing table. Event-triggering update indicates that BGP starts scanning and updates the routing table when the BGP configuration commands are changed due to user configuration or the next hop of a BGP route changes.

Configuration The following example configures the timely scan for the BGP protocol.

Examples Ruijie(config-router)# bgp scan-rib disable

	Command	Description
Related Commands	bgp scan-time	Configures the interval for the BGP timely scan.

Platform

Description None

5.45 bgp scan-time

Use this command to configure the interval for the BGP timely scan. Use the **no** or **default** form of this command to restore the default setting.

bgp scan-time *time*

no bgp scan-time [*time*]

default bgp scan-time [*time*]

Parameter	Description
<i>time</i>	Interval of the timely scan, in the range from 5 to 60 in the unit of seconds

Defaults The default is 60.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, or BGP Scope configuration mode.

Usage Guide This command is used to configure the interval for the BGP timely scan; it takes effect when `bgp scan-rib enable` is configured.

Configuration Examples The following example configures the interval for the BGP timely scan.

```
Ruijie(config-router)# bgp scan-time 30
```

Related Commands	Command	Description
	bgp scan-rib enable	Enables timely scan of the routing table by BGP.

Platform Description None

5.46 bgp tcp-source-check disable

Use this command to configure BGP's TCP source check function. Use **no** or **default** form of this command to disable this function.

bgp tcp-source-check disable

no bgp tcp-source-check disable

default bgp tcp-source-check disable

Parameter Description	Parameter	Description
	-	-

Defaults	This function is enabled by default.					
Command Mode	BGP configuration mode or BGP Scope Global configuration mode					
Usage Guide	After TCP source check function is disabled, all TCP connection requests will be received. After TCP connection is established, if no neighbor peer is configured on the local device, Notification packet will be send to refuse the BGP connection.					
Configuration Examples	The following example configures BGP's TCP source check function.					
Examples	<pre>Ruijie(config)# router bgp 65000 Ruijie(config-router)# bgp tcp-source-check disable</pre>					
Configuration Examples	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>router bgp</td> <td>Enables BGP protocol.</td> </tr> </tbody> </table>	Command	Description	router bgp	Enables BGP protocol.	
Command	Description					
router bgp	Enables BGP protocol.					
Platform	N/A					
Description						

5.47 bgp timer accuracy-control

Use this command to configure BGP's internal timer accuracy control. Use **no** or **default** form of this command to restore the default setting.

bgp timer accuracy-control
no bgp timer accuracy-control
default bgp timer accuracy-control

Parameter Description	Parameter	Description
	-	-

Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode	
Usage Guide	By default, a deviation from the given time will occur on the BGP protocol's timer to prevent concurrent overtime of many timers. You can use this command to configure BGP protocol's timer to strictly implement the given time. It is recommended disabling this function unless necessary.	
Configuration Examples	The following example configures BGP's internal timer accuracy control.	
Examples	<pre>Ruijie(config)# router bgp 65000 Ruijie(config-router)# bgp timer accuracy-control</pre>	

Configuration Examples	Command	Description
	<code>router bgp</code>	Enables BGP protocol.

Platform N/A

Description

5.48 bgp update-delay

Use this command to set the maximum delay time of the BGP Speaker before sending the first updating information to neighbors. The **no** or **default** form of the command restores it to the default value. During the BGP graceful-restart, this command is used to update the delay time.

bgp update-delay *delay-time*

no bgp update-delay

default bgp update-delay

Parameter	Description
<i>delay-time</i>	Maximum delay time of the BGP Speaker before sending its route updating information, in the range from 0 to 3600 in the unit of seconds, 120 seconds by default. For BGP graceful-restart, it is the maximum time of waiting to receive the EOR message of all neighbors, in the range from 1 to 3600 in the unit of seconds.

Defaults The default is 120.

Command

Mode BGP configuration mode or BGP Scope Global configuration mode

Usage Guide With the BGP starting up, it first waits some time to connect with its neighbors, and then sends the updating message to these neighbors. After connecting with neighbors, the BGP does not send the updating message to them immediately, but waits some time to receive the updating routing message from all neighbors and then performs routing optimization calculation and finally advertises the route updating message to its neighbors, which improves the convergence time and reduces the calculation consumption. If the software sends the route updating information to its neighbors immediately, it may send the information again when it receives more optimized routes from other neighbors.

The **bgp update-delay** command is used to adjust the initial waiting time of the software, which is the maximum time, from establishing the connection with the first neighbor to performing the routing optimization calculation and sending the route advertisement. When the BGP graceful-restart is enabled, this command is also used to set the maximum waiting time to receive EOR messages from all neighbors. You can increase this value if there are many neighbors or the routing information of the neighbors is huge. If the number of neighbors is 100 and the average amount of

routes is 5000, the update sending time that each neighbor completes all the routing is 1 second, then the update of all the routing needs 100 seconds; if the number of neighbors increases to 200, the Update Delay time can be set to 240 seconds, ensuring that all the routing can be updated with the Update Delay period. The specific time is also related to data transmission rate.

The following example sets the update-delay time to 200 seconds.

Configuration

```
Ruijie(config)# router bgp 500
```

Examples

```
Ruijie(config-router)# bgp graceful-restart
```

```
Ruijie(config-router)# bgp update-delay 200
```

Related

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Commands**Platform**

Description None

5.49 bgp upgrade-cli

Use this command to set the BGP CLI display mode. Use the **no** or **default** form of this command to restore the default setting.

bgp upgrade-cli { af-mode | scope-mode }

no bgp upgrade-cli { af-mode | scope-mode }

default bgp upgrade-cli { af-mode | scope-mode }

Parameter

Parameter	Description
af-mode	CLI is displayed in address family configuration mode.
scope-mode	CLI is displayed in scope configuration mode.

Description**Defaults**

The default is **af-mode**. When you execute the **scope** command, the display mode is switched to scope configuration mode automatically.

Command

Mode BGP configuration mode/ BGP scope global configuration mode.

Usage**Guide**

When the display mode is switched to the scope global configuration mode, all CLI commands will be displayed either in the scope configuration mode or the address-family mode that under the scope configuration mode.

Configuration

The following example sets the scope global configuration mode as the BGP CLI display mode.

Examples

```
Ruijie(config)# router bgp 500
```

```
Ruijie(config-router)# bgp upgrade-cli scope-mode
```

Related

Command	Description
---------	-------------

Commands	N/A	N/A
-----------------	-----	-----

Platform

Description N/A

5.50 clear bgp all

Use this command to reset all BGP address-families. The content to be reset depends on the further parameters .

clear bgp all [*as number*] [**soft**] [**in** | **out**]

	Parameter	Description
Parameter Description	<i>none parameter</i>	Resets peer sessions in all address-families.
	<i>as-number</i>	Resets sessions with all members in the specified AS. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.
	in	Soft-resets the received routing information.
	out	Soft-resets the redistributed routing information.
	soft	Soft-resets all routing information received/sent from/to the specified peer.
	soft in	Soft-resets the received routing information.
	soft out	Soft-resets the distributed routing information.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage This command is used to reset sessions of all supported address-families, including the vrf session
Guide in every address-family.

Configuration

Examples N/A

	Command	Description
Related Commands	clear bgp ipv4 unicast	Resets the IPv4 unicast address-family.

Platform

Description None

5.51 clear bgp all peer-group

Use this command to reset BGP's specific peer group. The reset content is determined by further parameters.

clear bgp all peer-group *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	<i>peer-group-name</i>	Resets a specific peer group.
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide This command will reset replies of all supported address families, including reply connection included in vrf in each address family.

Configuration Examples -

Configuration Examples	Command	Description
	clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.

Platform -

Description

5.52 clear bgp ipv4 unicast

Use this command to reset BGP IPv4 unicast address families. The reset content is determined by further parameters.

clear bgp ipv4 unicast [**vrf** *vrf-name*] { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	*	Resets all peer group sessions under address families.

<i>as-number</i>	Resets sessions with all members in the specified AS.
<i>peer-address</i>	Resets sessions with the specified peer.
in	Soft-resets received route information.
out	Soft-resets allocated route information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is the same as **clear ip bgp** in terms of the function and parameters.

Configuration Examples N/A

Configuration Examples	Command	Description
	N/A	N/A

Platform N/A

Description

5.53 clear bgp ipv4 unicast dampening

Use this command to clear the flap information and disable route dampening.

clear bgp ipv4 unicast [vrf *vrf-name*] dampening [*ip-address* [*mask*]]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
	-	Clears the flap information of all routes.
	<i>address</i>	IP address
	<i>mask</i>	Mask

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the BGP route dampening information and release suppressed routes. This command can be used to restart the BGP route dampening.

Configuration The following example clears the flap information and disables route dampening.

Examples

```
Ruijie# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

	Command	Description
Related Commands	show ip bgp dampening dampened-paths	Displays the suppressed routing information.
	bgp dampening	Enables the route dampening and sets the dampening parameters.

Platform

Description None

5.54 clear bgp ipv4 unicast external

Use this command to reset all EBGp connections.

clear bgp ipv4 unicast [vrf *vrf-name*] external [soft] [in | out]

	Parameter	Description
Parameter Description	<i>vrf-name</i>	VRF name.
	in	Without parameter soft, resets the session of the peer to establish active connection.
	out	Without parameter soft, resets the session of the local BGP speaker to establish active connection.
	soft	Soft-resets all routing information received/sent from/to the specified peer.
	soft in	Soft-resets the received routing information.
	soft out	Soft-resets the distributed routing information.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

Guide This command is used to reset the specified external BGP connection.

Configuration The following example resets all EBGp connections.

Examples

```
Ruijie# clear bgp ipv4 unicast external in
```

	Command	Description
Related Commands	clear ip bgp	Resets the BGP session.
	show ip bgp neighbors	Displays the neighbor information.

Platform
Description None

5.55 clear bgp ipv4 unicast flap-statistics

Use this command to clear the route flap information.

clear bgp ipv4 unicast [vrf *vrf-name*] flap-statistics [*address* [*mask*]]

Parameter
Description

Parameter	Description
<i>vrf-name</i>	VRF name.
-	Clears all route flap information
<i>address</i>	IP address
<i>mask</i>	Mask

Defaults N/A

Command

Mode Privileged EXEC mode

Usage
Guide

This command can be used only to clear the statistics of unsuppressed routes. It does not release the suppressed routes. To clear all route statistics and release the suppressed routes, run the **clear ip bgp dampening** command.

Configuration The following example clears the route flap information.

Examples Ruijie# clear bgp ipv4 unicast flap-statistics

Related
Commands

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.
show ip bgp	Displays the BGP route entry.

Platform

Description None

5.56 clear bgp ipv4 unicast peer-group

Use this command to reset the session with all members in the peer group.

clear bgp ipv4 unicast [vrf *vrf-name*] peer-group *peer-group-name* [*soft*] [in | out]

Parameter
Description

Parameter	Description
<i>vrf-name</i>	VRF name
<i>peer-group-name</i>	Name of the peer group

in	Without parameter soft, resets the session of the peer to establish active connection.
out	Without parameter soft, resets the session of the local BGP speaker to establish active connection.
soft	Soft-resets all routing information received/sent from/to the specified peer.
soft in	Soft-resets for the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

Guide This command resets the BGP session with all members in the peer group.

Configuration The following example resets the session with all members in the peer group.

Examples Ruijie# clear bgp ipv4 unicast peer-group my-group in

Related Commands	Command	Description
	clear ip bgp	Resets the BGP session.
	show ip bgp	Displays the BGP route entry.

Platform

Description None

5.57 clear bgp ipv4 unicast table-map

Use this command to update the table-map setting under the IPv4 unicast address family of BGP.

clear bgp ipv4 unicast [vrf *vrf-name*] table-map

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name

Defaults -

Command Privileged EXEC mode

Mode

Usage Guide Re-apply table-map setting and update allocated core route table information.

Configuration -

Examples

Parameter Description	Command	Description
	clear ip bgp	Resets BGP's IPv4 unicast address families.

Platform -

Description

5.58 clear bgp ipv6 unicast

Use this command to reset BGP's IPv6 unicast address families.

clear bgp ipv6 unicast [*vrf vrf-name*] { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	*	Resets all peer group sessions under address families.
	<i>as-number</i>	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.
	<i>peer-address</i>	Resets sessions with the specified peer.
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults -

Command Privileged EXEC mode

Mode

Usage Guide The function is similar with **clear bgp ipv4 unicast**, but applies to different address families.

Configuration -

Examples

Configuration	Command	Description
---------------	---------	-------------

Examples		
	<code>clear bgp ipv4 unicast</code>	Resets BGP's IPv4 unicast address families.

Platform -

Description

5.59 clear bgp ipv6 unicast dampening

Use this command to clear flap information and disable route dampening.

`clear bgp ipv6 unicast [vrf vrf-name] dampening [ip-address [mask]]`

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	-	Clears all routes' flap information.
	<i>ip-address</i>	IP address
	<i>mask</i>	Mask code

Defaults -

Command Privileged EXEC mode

Mode

Usage Guide You can use this command to clear BGP's route flap information and disable route dampening. The command can restart BGP's route flap.

Configuration The following example clears flap information and disables route dampening.

Examples Ruijie# `clear bgp ipv6 unicast dampening 192.168.0.0 255.255.0.0`

Configuration Examples	Command	Description
	<code>bgp dampening</code>	Enables the route dampening function and sets dampening parameters.

Platform -

Description

5.60 clear bgp ipv6 unicast external

Use this command to reset all EBGP connection of IPv6 unicast address families.

clear bgp ipv6 unicast [vrf *vrf-name*] external [soft] [in | out]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide You can use this command to reset all the specified external BGP connection.

Configuration Examples The following example resets all EBGp connection of IPv6 unicast address families.

Examples Ruijie# clear bgp ipv6 unicast external in

Configuration Examples	Command	Description
	clear ip bgp	Resets BGP sessions.
	show ip bgp neighbors	Displays BGP neighbors' information.

Platform -

Description

5.61 clear bgp ipv6 unicast flap-statistics

Use this command to clear IPv6 unicast address families' route flap statistics.

clear bgp ipv6 unicast [vrf *vrf-name*] flap-statistics [address [mask]]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	-	Clears all route information's flap information.
	<i>address</i>	IP address
	<i>mask</i>	Mask code

Defaults -

Command Privileged EXEC mode
Mode

Usage Guide This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the **clear bgp ipv4 unicast dampening** command.

Configuration The following example clears IPv6 unicast address families' route flap statistics.

Examples Ruijie# clear bgp ipv6 unicast flap-statistics

Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
	show ip bgp	Displays BGP route entries.

Platform -
Description

5.62 clear bgp ipv6 unicast peer-group

Use this command to reset sessions with all members in the peer group.

clear bgp ipv6 unicast [*vrf vrf-name*] **peer-group** *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	<i>peer-group-name</i>	Peer group name
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults -

Command Privileged EXEC mode
Mode

Usage Guide Use this command to reset BGP sessions with all members in the peer group.

Configuration The following example resets sessions with all members in the peer group.

Examples Ruijie# clear bgp ipv6 unicast peer-group my-group in

Configuration

Examples

Command	Description
clear ip bgp	Resets BGP sessions.
show ip bgp	Displays BGP route entries.

Platform

-

Description

5.63 clear bgp ipv6 unicast table-map

Use this command to update the table-map setting under the IPv6 unicast address family of BGP.

clear bgp ipv6 unicast [vrf *vrf-name*] table-map

Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name

Defaults -

Command Mode Privileged EXEC mode

Usage Guide -

Configuration -

Examples

Configuration Examples	Command	Description
	clear ip bgp	Resets BGP's IPv4 unicast address families.

Platform -

Description

5.64 clear bgp l2vpn vpls

Use this command to reset BGP EVPN address families.

clear bgp l2vpn evpn { * | *as-number* | *peer-address* } [**soft] [**in** | **out**]**

Parameter Description	Parameter	Description
	*	Resets all peer group sessions under address families.
	<i>as-number</i>	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.
	<i>peer-address</i>	Resets sessions with the specified peer.
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.

soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide The function is similar with **clear bgp ipv4 unicast**, but applies to different address families.

Configuration -

Examples

Configuration Examples	Command	Description
	clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.

Platform -

Description

5.65 clear bgp l2vpn evpn dampening

Use this command to clear flap information and disable route dampening.

clear bgp l2vpn evpn dampening

Parameter Description	Parameter	Description
	N/A	N/A

Defaults -

Command Mode Privileged EXEC mode

Usage Guide You can use this command to clear BGP's route flap information and relieve damped routes. The command can restart BGP's route flap.

Configuration The following example clears flap information and disables route dampening.

Examples Ruijie# clear bgp l2vpn evpn dampening

Platform N/A

Description

5.66 clear bgp l2vpn evpn external

Use this command to reset all EBGp connection of BGP EVPN address families.

clear bgp l2vpn evpn external [soft] [in | out]

Parameter Description	Parameter	Description
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to reset all the specified external BGP connection.

Configuration The following example resets all EBGp connection of L2VPN EVPN address families.

Examples Ruijie# clear bgp l2vpn evpn external in

Platform Description N/A

5.67 clear bgp l2vpn evpn flap-statistics

Use this command to clear BGP EVPN address families' route flap statistics.

clear bgp l2vpn evpn flap-statistics

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the clear bgp l2vpn evpn dampening command.	
Configuration Examples	The following example clears L2VPN EVPN address families' route flap statistics.	
Examples	<pre>Ruijie# clear bgp l2vpn evpn flap-statistics</pre>	
Platform Description	N/A	

5.68 clear bgp l2vpn evpn peer-group

Use this command to reset sessions of all members in the peer group.

clear bgp l2vpn evpn peer-group *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	<i>peer-group-name</i>	Peer group name
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide Use this command to reset BGP sessions of all members in the peer group.

Configuration Examples The following example displays that the L2VPN EVPN address family soft-resets received route information of all members in the peer group my-group.

```
Ruijie# clear bgp l2vpn evpn peer-group my-group in
```

Platform N/A

Description

5.69 clear bgp l2vpn vpls

Use this command to reset BGP VPLS address families.

clear bgp l2vpn vpls { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	*	Resets all peer group sessions under address families.
	<i>as-number</i>	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.
	<i>peer-address</i>	Resets sessions with the specified peer.
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide The function is similar with **clear bgp ipv4 unicast**, but applies to different address families.

Configuration Examples -

Configuration Examples	Command	Description
	clear bgp ipv4 unicast	Resets BGP IPv4 unicast address families.

Platform -
Description

5.70 clear bgp l2vpn vpls dampening

Use this command to clear flap information and disable route dampening.

clear bgp l2vpn vpls dampening [*ve_id:offset*]

Parameter Description	Parameter	Description
	-	Clears all routes' flap information.
	<i>ve_id:offset</i>	Clears specified <i>ve_id:offset</i> 's vfi instance route flap information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide You can use this command to clear BGP's route flap information and relieve damped routes. The command can restart BGP's route flap.

Configuration Examples The following example clears flap information and disables route dampening.

```
Ruijie# clear bgp l2vpn vpls dampening
```

Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform -
Description

5.71 clear bgp l2vpn vpls external

Use this command to reset all EBGp connection of BGP VPLS address families.

clear bgp l2vpn vpls external [*soft*] [*in* | *out*]

Parameter Description	Parameter	Description
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.

soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Privileged EXEC mode

Mode

Usage Guide You can use this command to reset all the specified external BGP connection.

Configuration The following example resets all EBGp connection of BGP VPLS address families.

Examples Ruijie# clear bgp l2vpn vpls external in

Configuration Examples	Command	Description
	clear ip bgp	Resets BGP sessions.
show ip bgp neighbors	Displays BGP neighbors' information.	

Platform -

Description

5.72 clear bgp l2vpn vpls flap-statistics

Use this command to clear BGP VPLS address families' route flap statistics.

clear bgp l2vpn vpls flap-statistics [*ve_id:offset*]

Parameter Description	Parameter	Description
	-	Clears all routes' flap information.
	<i>ve_id:offset</i>	Clears specified <i>ve_id:offset</i> 's vfi instance route flap information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the **clear bgp l2vpn vpls dampening** command.

Configuration Examples The following example clears BGP VPLS address families' route flap statistics.

Examples Ruijie# clear bgp l2vpn vpls flap-statistics

Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
	show ip bgp	Displays BGP route entries.

Platform -

Description

5.73 clear bgp l2vpn vpls peer-group

Use this command to reset sessions of all members in the peer group.

clear bgp l2vpn vpls peer-group *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	<i>peer-group-name</i>	Peer group name
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.

soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Privileged EXEC mode

Mode

Usage Guide Use this command to reset BGP sessions of all members in the peer group.

Configuration Examples The following example displays that the L2VPN VPLS address family soft-resets received route information of all members in the peer group my-group.

```
Ruijie# clear bgp l2vpn vpls peer-group my-group in
```

Configuration Examples

Command	Description
clear ip bgp	Resets BGP sessions.
show ip bgp	Displays BGP route entries.

Platform -

Description

5.74 clear bgp l2vpn vpws

Use this command to reset BGP's VPWS address families.

```
clear bgp l2vpn vpws { * | as-number | peer-address } [ soft ] [ in | out ]
```

Parameter Description

Parameter	Description
*	Resets all peer group sessions under address families.
<i>as-number</i>	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.
<i>peer-address</i>	Resets sessions with the specified peer.
in	Soft-resets received route information.
out	Soft-resets allocated route information.
soft	Soft-resets received and sent route information.
soft in	Soft-resets received route information.
soft out	Soft-resets allocated route information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide The function is similar with **clear bgp ipv4 unicast**, but applies to different address families.

Configuration Examples -

Configuration Examples	Command	Description
	clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.

Platform Description -

5.75 clear bgp l2vpn vpws dampening

Use this command to clear flap information and disable route dampening.

clear bgp l2vpn vpws dampening [*ve_id:offset*]

Parameter Description	Parameter	Description
	-	Clears all routes' flap information.
	<i>ve_id:offset</i>	Clears specified <i>ve_id:offset</i> 's vfi instance route flap information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide You can use this command to clear BGP's route flap information and relieve damped routes. The command can restart BGP's route flap.

Configuration Examples The following example clears flap information and disables route dampening.

Examples Ruijie# clear bgp l2vpn vpws dampening

Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform Description -

5.76 clear bgp l2vpn vpws external

Use this command to reset all EBGP connection of BGP VPWS address families.

clear bgp l2vpn vpws external [soft] [in | out]

Parameter Description	Parameter	Description
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide You can use this command to reset all the specified external BGP connection.

Configuration Examples The following example resets all EBGP connection of BGP VPWS address families.

Examples Ruijie# clear bgp l2vpn vpws external in

Configuration Examples	Command	Description
	clear ip bgp	Resets BGP sessions.
	show ip bgp neighbors	Displays BGP neighbors' information.

Platform -

Description

5.77 clear bgp l2vpn vpws flap-statistics

Use this command to clear BGP VPWS address families' route flap statistics.

clear bgp l2vpn vpws flap-statistics [ve_id:offset]

Parameter Description	Parameter	Description
	-	Clears all routes' flap information.
	<i>ve_id:offset</i>	Clears specified <i>ve_id:offset</i> 's vfi instance route flap information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the **clear bgp l2vpn vpws dampening** command.

Configuration Examples The following example clears BGP VPWS address families' route flap statistics.

```
Ruijie# clear bgp l2vpn vpws flap-statistics
```

Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
show ip bgp	Displays BGP route entries.	

Platform -

Description

5.78 clear bgp l2vpn vpws peer-group

Use this command to reset sessions with all members in the peer group.

```
clear bgp l2vpn vpws peer-group peer-group-name [ soft ] [ in | out ]
```

Parameter Description	Parameter	Description
	<i>peer-group-name</i>	Peer group name
in	Soft-resets received route information.	
out	Soft-resets allocated route information.	
soft	Soft-resets received and sent route information.	
soft in	Soft-resets received route information.	
soft out	Soft-resets allocated route information.	

Defaults -

Command Mode Privileged EXEC mode

Usage Guide Use this command to reset BGP sessions with all members in the peer group.

Configuration Examples The following example resets sessions with all members in the peer group.

```
Ruijie# clear bgp l2vpn vpws peer-group my-group in
```


Configuration Examples	Command	Description
	<code>clear ip bgp</code>	Resets BGP sessions.
<code>show ip bgp</code>	Displays BGP route entries.	

Platform -

Description

5.79 clear bgp vpnv4 unicast

Use this command to reset BGP's VPNV4 unicast address families.

clear bgp vpnv4 unicast { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	*	Resets all peer group sessions under address families.
<i>as-number</i>	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.	
<i>peer-address</i>	Resets sessions with the specified peer.	
in	Soft-resets received route information.	
out	Soft-resets allocated route information.	
soft	Soft-resets received and sent route information.	
soft in	Soft-resets received route information.	
soft out	Soft-resets allocated route information.	

Defaults -

Command Privileged EXEC mode

Mode

Usage Guide The function is similar with **clear bgp ipv4 unicast**, but applies to different address families.

Configuration -

Examples

Configuration Examples	Command	Description
	<code>clear bgp ipv4 unicast</code>	Resets BGP's IPv4 unicast address families.

Platform -

Description

5.80 clear bgp vpnv4 unicast dampening

Use this command to clear flap information and disable route dampening.

clear bgp vpnv4 unicast dampening [*ip-address* [*mask*]]

Parameter Description	Parameter	Description
	-	Clears all routes' flap information.
	<i>ip-address</i>	IP address
	<i>mask</i>	Mask code

Defaults -

Command Mode Privileged EXEC mode

Usage Guide You can use this command to clear BGP's route flap information and relieve damped routes. The command can restart BGP's route flap.

Configuration Examples The following example clears flap information and disables route dampening.

```
Ruijie# clear bgp vpnv4 unicast dampening
```

Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform -

Description

5.81 clear bgp vpnv4 unicast external

Use this command to reset all EBGp connection of VPNv4 address families.

clear bgp vpnv4 unicast external [*soft*] [*in* | *out*]

Parameter Description	Parameter	Description
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults	-
Command Mode	Privileged EXEC mode
Usage Guide	You can use this command to reset all the specified external BGP connection.
Configuration Examples	The following example resets all EBGp connection of VPNv4 address families.
Examples	Ruijie# clear bgp vpnv4 unicast external in

Configuration Examples	Command	Description
	clear ip bgp	Resets BGP sessions.
	show ip bgp neighbors	Displays BGP neighbors' information.

Platform	-
Description	

5.82 clear bgp vpnv4 unicast flap-statistics

Use this command to clear VPNv4 address families' route flap statistics.

clear bgp vpnv4 unicast flap-statistics [*ip-address* [*mask*]]

Parameter Description	Parameter	Description
	-	Clears all routes' flap information.
	<i>ip-address</i>	IP address
	<i>mask</i>	Mask code

Defaults	-
Command Mode	Privileged EXEC mode
Usage Guide	This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the clear bgp vpnv4 unicast dampening command.
Configuration Examples	The following example clears VPNv4 address families' route flap statistics.
Examples	Ruijie# clear bgp vpnv4 unicast flap-statistics

Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
	show ip bgp	Displays BGP route entries.

Platform -

Description

5.83 clear bgp vpnv4 unicast peer-group

Use this command to reset sessions with all members in the peer group.

clear bgp vpnv4 unicast peer-group *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
		<i>peer-group-name</i>
	in	Soft-resets received route information.
	out	Soft-resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.

Defaults -

Command Privileged EXEC mode
Mode

Usage Guide Use this command to reset BGP sessions with all members in the peer group.

Configuration The following example resets sessions with all members in the peer group.

Examples Ruijie# clear bgp vpnv4 unicast peer-group my-group in

Configuration Examples	Command	Description
	clear ip bgp	Resets BGP sessions.
	show ip bgp	Displays BGP route entries.

Platform -

Description

5.84 clear ip bgp

Use this command to reset the BGP session.

clear ip bgp [vrf *vrf-name*] { * | *as-number* / *peer-address* } [soft] [in | out]

Parameter	Description
<i>vrf-name</i>	VRF name.
*	Resets all the current BGP sessions and the OVERFLOW status of BGP ipv4 unicast address family.
<i>address</i>	Resets the BGP session with the specified peer.
<i>as number</i>	Resets sessions with all members in the specified AS. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.
in	Soft-reset the received routing information.
out	Soft-reset the redistributed routing information.
soft	Soft-reset all routing information received/sent from/to the specified peer
soft in	Soft-reset the received routing information.
soft out	Soft-reset the distributed routing information.

Parameter Description

Defaults N/A

Command

Mode Privileged EXEC mode


At any time, once the routing policy or BGP configuration changes, an effective way must be available to implement the new routing policy or configuration. Traditional measure is to close the BGP connection and establish a new one.

This product supports implementing a new routing strategy without closing the BGP session connection by soft-resetting BGP.

Usage Guide

For the peer that does not support the route refresh function, you may run the **neighbor soft-reconfiguration inbound** command to keep a copy of original routing information of every specified BGP peer on the local BGP speaker. This will consume some resources.

You can use the **show ip bgp neighbors** command to see whether the BGP peer supports the route refresh function. If it is supported, you need not to execute the **neighbor soft-reconfiguration inbound** command when the inbound routing strategy changes.

 All connected BGP routers must support the route refresh function to execute this command. This product supports the route refresh function.

Configuration The following example resets the BGP session.

Examples

```
Ruijie# clear bgp ipv4 unicast *
```

**Related
Commands**

Command	Description
neighbor soft-reconfiguration inbound	(Optional) Restarts the BGP session and reserves the unchanged route information sent by the BGP peer (group).
show ip bgp	Displays the BGP route entry.

Platform

Description None

5.85 clear ip bgp dampening

Use this command to clear the dampening information and disable route dampening.

```
clear ip bgp [ vrf vrf-name ] dampening [ ip-address [ mask ] ]
```

**Parameter
Description**

Parameter	Description
<i>vrf-name</i>	VRF name
<i>address</i>	IP address
<i>mask</i>	Mask

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

This command is used to clear the BGP route flap information and disable route dampening. This command can be used to restart BGP route dampening.

Guide**Configuration**

The following example clears the dampening information and disables route dampening.

Examples

```
Ruijie# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

**Related
Commands**

Command	Description
show ip bgp dampening dampened-paths	Displays the suppressed routing information.
bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform

Description None

5.86 clear ip bgp external

Use this command to reset all EBGp connections.

clear ip bgp [vrf *vrf-name*] external [soft] [in | out]

Parameter	Description
<i>vrf-name</i>	VRF name.
in	Without parameter soft, resets the session through which the peer establishes active connection.
out	Without parameter soft, resets the session through which the local BGP speaker establishes active connection.
soft in	Soft-resets the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

Guide This command is used to reset the specified external BGP connection.

Configuration The following example resets all EBGp connections.

Examples Ruijie# clear ip bgp external in

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp neighbors	Displays the neighbor information.

Platform

Description None

5.87 clear ip bgp flap-statistics

Use this command to clear the routes vibration statistics of the IPv4 unicast address family.

clear ip bgp [vrf *vrf-name*] flap-statistics [ip-address [mask]]

Parameter	Description
<i>vrf-name</i>	VRF name.
<i>address</i>	IP address
<i>Mask</i>	Mask

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

Guide

This command can be used only to clear statistics of unsuppressed routes. It does not release the suppressed routes. To clear all route statistics and release the suppressed routes, run the **clear ip bgp dampening** command.

Configuration

The following example clears the routes vibration statistics of the IPv4 unicast address family.

Examples

```
Ruijie# clear ip bgp flap-statistics
```

Related

Commands

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.
show ip bgp	Displays the BGP route entry.

Platform

Description None

5.88 clear ip bgp peer-group

Use this command to reset the session with all members in the peer group.

clear ip bgp [vrf *vrf-name*] peer-group *peer-group-name* [soft] [in | out]

Parameter

Description

Parameter	Description
<i>vrf-name</i>	VRF name.
<i>peer-group-name</i>	Name of the peer group
in	Without parameter soft , resets the session through which the peer establishes active connection.
out	Without parameter soft , resets the session through which the local BGP speaker establishes active connection.
soft	Soft-resets all routing information received/sent from/to the specified peer
soft in	Soft-resets the received routing information.
soft out	Soft-resets the distributed routing information.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

This command resets the BGP session with all members in the peer group.

Guide

Configuration The following example resets the session with all members in the peer group.

Examples Ruijie# clear ip bgp peer-group my-group in

**Related
Commands**

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Displays the BGP route entry.

Platform

Description None

5.89 clear ip bgp table-map

Use this command to update the table-map's route information applied by IPv4 unicast address family.

clear ip bgp [vrf *vrf-name*] table-map

Parameter	Parameter	Description
Description	<i>vrf-name</i>	vrf name

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

Guide This command is used to update the route information of the applied table-map.

Configuration The following example updates the table-map's route information applied by IPv4 unicast address family.

Examples Ruijie# clear ip bgp table-map

**Related
Commands**

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Displays the BGP route entry.

Platform

Description None

5.90 default-information originate

Use this command to enable BGP to distribute the default route. Use the **no** form of this command to restore the default setting.

default-information originate

[no] default-information originate

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, BGP IPv4 VRF configuration mode, BGP IPv6 VRF configuration mode

Usage Guide This command is used to control whether the redistributed default route is effective, and this command needs to be configured together with the **redistribute** command. It takes effect only when a default route exists in the redistributed route.

This command is similar to the **network** command. The difference is that in the process of configuring the former, the **redistribute** command must be configured explicitly to redistribute the default route, only in this case, the redistributed default route is effective. For the later command, the IGP must have the default route.

Configuration Examples The following example enables BGP to distribute the default route.

```
Ruijie(config-router)# default-information originate
```

Related Commands	Command	Description
	network	Configures routes to be advertised.
	redistribute	Redistributes routes of other protocol.

Platform Description None

5.91 default-metric


Use this command to set the metric for route redistribution. Use the **no** or **default** form of this command to restore the default setting.

default-metric *number*

no default-metric

default default-metric

Parameter	Parameter	Description
-----------	-----------	-------------

Description	<i>number</i>	Metric number, in the range from 1 to 4294967295				
Defaults	No metric is set by default.					
Command Mode	BGP configuration mode, BGP IPv4/ IPv6 Unicast address family configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode or BGP Scope configuration mode.					
Usage Guide	This command sets the metric of routes to be redistributed for integrity.					
Usage Guide	<p> The metric set by the command cannot cover that set by the redistribute metric command. The value is 0 when the default metric applies to redistributed connected routes.</p>					
Configuration Examples	The following example sets the metric for route redistribution.					
Configuration Examples	<pre>Ruijie(config-router)# default-metric 45</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>redistribute</td> <td>Redistributes routes of other protocol.</td> </tr> </tbody> </table>	Command	Description	redistribute	Redistributes routes of other protocol.	
Command	Description					
redistribute	Redistributes routes of other protocol.					
Platform Description	None					

5.92 distance bgp

Use this command to set different management distances for different types of BGP routes. Use the **no** or **default** form of this command to restore the default setting.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

default distance bgp

Parameter	Description
<i>external-distance</i>	Route management distance learned from EBGp peers, in the range from 1 to 255
<i>internal-distance</i>	Route management distance learned from IBGP peers, in the range from 1 to 255
<i>local-distance</i>	Specifies the management distance of route learned from peers. However, the optimal one can be learned from the IGP. In general, these routes are indicated by the Network Backdoor command. The value is in the range from 1 to 255

The parameter defaults are as follows:

Defaults

external-distance - 20
internal-distance - 200

local-distance - 200

Command

Mode BGP configuration mode or BGP Scope configuration mode.

It is not recommended to change the management distance of the BGP route. If it is necessary, observe the following points:

- Usage Guide**
- The management distance of "external-distance" must be shorter than those of other IGP routing protocols (such as OSPF and RIP);
 - The internal-distance and local-distance should have longer management distances than other IGP routing protocols.

Configuration Examples The following example sets different management distances for different types of BGP routes.

```
Ruijie(config-router)# distance bgp 20 20 200
```

Related Commands

Command	Description
neighbor soft-reconfiguration inbound	Restarts the BGP session and reserves the unchanged route information sent by the BGP peer (group).
show ip bgp	Displays the BGP route entry.

Platform

Description None

5.93 exit-address-family

Use this command to exit BGP address-family configuration mode.

exit-address-family

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command

Mode BGP address-family configuration mode

Usage Guide This command can be used to exit from various address-family modes of BGP to BGP configuration mode.

Configuration Examples The following example exits the BGP address-family configuration mode.

```
Ruijie(config-router-af)#exit-address-family
```

Related

Command	Description
---------	-------------

Commands	address-family ipv4	Enters IPv4 address family configuration mode.
-----------------	----------------------------	--

Platform

Description None

5.94 maximum-paths ebgp

Use this command to configure the number of cost-equal paths for the EBGp multipathing load balancing function. Use the **no** or **default** form of this command to restore the default setting.

maximum-paths ebgp *number*

no maximum-paths ebgp

default maximum-paths ebgp

**Parameter
Description**

Parameter	Description
<i>number</i>	Maximum number of cost-equal paths The parameter value ranges from 1 to 32. When the parameter is set to 1, the EBGp multipathing load balancing function is disabled.

Defaults EBGp multipathing load balancing is disabled by default.

Command Mode BGP configuration mode/ BGP IPv4 unicast address configuration mode/ BGP IPv6 unicast address-family configuration mode/ BGP scope global configuration mode

Usage Guide When EBGp ECMP must be supported, run the maximum-paths ebgp command to configure the maximum number of cost-equal paths. The command also applies to EBGp ECMP in the confederation.

Configuration Examples The following example configures the number of cost-equal paths for the EBGp multipathing load balancing function.

```
Ruijie(config)# router bgp 65530
Ruijie(config-router)# maximum-paths ebgp 2
```

**Related
Commands**

Command	Description
router bgp	Enables BGP.
show ip bgp	Displays BGP routing entries.

Platform N/A

Description

5.95 maximum-paths ibgp

Use this command to configure the number of cost-equal paths for the IBGP multipathing load balancing function. Use the **no** or **default** form of this command to disable the IBGP multipathing load balancing function.

maximum-paths ibgp *number*

no maximum-paths ibgp

default maximum-paths ibgp

Parameter	Parameter	Description
Description	<i>number</i>	Maximum number of cost-equal paths The parameter value ranges from 1 to 32. When the parameter is set to 1, the IBGP multipathing load balancing function is disabled.

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/ IPv6 Unicast address family configuration mode or BGP Scope Global configuration mode

Usage Guide When IBGP ECMP must be supported, run the maximum-paths ibgp command to configure the maximum number of cost-equal paths.

Configuration Examples The following example configures the number of cost-equal paths for the IBGP multipathing load balancing function.

```
Ruijie(config)# router bgp 65530
Ruijie(config-router)# maximum-paths ibgp 2
```

Related Commands	Command	Description
	router bgp	Enables BGP.
	show ip bgp	Displays BGP routing entries.

Platform N/A

Description

5.96 maximum-prefix

Use this command to limit the maximum number of prefixes in the routing database in the address family. Use the **no** or **default** form of this command to restore the default setting.

maximum-prefix *maximum*

no maximum-prefix [*maximum*]

default maximum-prefix [*maximum*]

	Parameter	Description
Parameter Description	<i>maximum</i>	The maximum number of prefixes in the routing database in the address family, in the range from 1 to 4294967295
	no	Restores the default maximum number.

Defaults

The default maximum numbers of prefixes in the routing database vary with address families. The default number in the IPv4 VRF, IPv6 VRF, IPv4 Multicast, IPv6 Multicast, IPv4 MDT address family is 10000; The default number in the other address family is 4294967295.

Command Mode


BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.


In a BGP address family, routing prefixes may be introduced through redistribution or learnt from neighbors, or other VRFs. Once routing prefixes in the BGP address family reaches the maximum number, this address family will enter to the overflow state.

Use the **show bgp { addressfamily | all } summary** command to display the state of routing database.

It is necessary to reconfigure BGP for state clearing, or use the **clear bgp { addressfamily | all } *** command to reset the address family.

Usage Guide

 When the address family is overflow as the number of prefixes reaches the maximum number, you can adjust maximum-prefix.

 Maximum-prefix will not filter the routing information generated by the network and aggregate commands.

IPv4 unicast routes can receive the routing prefix in the following conditions even in the Overflow state:

- The route information of the same routing prefix exists in the address database.
- One route that overwrites this prefix (except for the default route) exists in the address database and the next-hop of this route is different from that of the newly received routing prefix.

Configuration Examples

The following example sets the maximum number of prefixes in the BGP routing database in the ipv4 multicast address family.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv4 multicast
Ruijie(config-router-af)# maximum-prefix 65535
```

Related Commands

Command	Description
clear bgp all	Resets BGP's all address families.
clear bgp ipv4 mdt	Resets BGP's ipv4 mdt address families.
clear bgp ipv4 unicast	Resets BGP's ipv4 unicast address families.

clear bgp ipv6 unicast	Resets BGP's ipv6 unicast address families.
clear bgp vpv4 unicast	Resets BGP's vpv4 unicast address families.
show bgp all summary	Displays summary of BGP's all address families.
show bgp ipv4 mdt summary	Displays summary of BGP's ipv4 mdt address families.
show bgp ipv4 unicast summary	Displays summary of BGP's ipv4 unicast address families.
show bgp ipv6 unicast summary	Displays summary of BGP's ipv6 unicast address families.
show bgp vpv4 summary	Displays summary of BGP's vpv4 unicast address families.

Platform**Description** N/A

5.97 neighbor activate

Use this command to activate the neighbor or peer group in the current address mode. Use the **no** or **default** form of this command to disable this function.

neighbor {peer-address | peer-group-name} activate

no neighbor {peer-address | peer-group-name} activate

default neighbor { peer-address | peer-group-name } activate

	Parameter	Description
Parameter Description	<i>peer-address</i>	IP address of the peer, IPv4 address or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults This function is enabled in IPv4 address family mode by default.

Command Mode BGP configuration mode, BGP IPv4/ IPv6 Unicast address family configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode, or BGP Scope configuration mode.

Usage Guide The function is enabled by default for IPv4 address families. You need to set this command in other address-family configuration modes for exchanging routes.

The following example activates the neighbor or peer group in the current address mode.

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router)# address-family vpv4
Ruijie(config-router-af)# neighbor 10.0.0.1 activate
```


Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.

Platform	
Description	None

5.98 neighbor advertisement-interval

Use this command to set the time interval to send the BGP route update message. Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} advertisement-interval seconds

no neighbor {peer-address | peer-group-name} advertisement-interval

default neighbor { peer-address | peer-group-name } advertisement-interval

Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>seconds</i>	Time interval to send the route update message in the range from 0 to 600 seconds

Defaults	IBGP connection: 15 seconds EBGP connection: 30 seconds
----------	--

Command Mode	BGP configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode or BGP Scope configuration mode.
-----------------	---

Usage Guide	If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command.
----------------	---

The following example sets the time interval to send the BGP route update message.

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router)# neighbor 10.0.0.1 advertisement-interval 10
```

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.

Platform	
Description	None

5.99 neighbor allowas-in

Use this command to allow the PE to receive messages with the same AS number as itself. Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} allowas-in number

no neighbor {peer-address | peer-group-name} allowas-in

default neighbor { peer-address | peer-group-name } allowas-in

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>number</i>	Number of the AS number duplication in the range from 1 to 10, 3 by default

Parameter Description

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

A typical application is spoke_hub mode. Execute this command on the PE to enable it to receive and then send the advertised address prefix. Configure two VRFs on the PE. One VRF receives the routes of all PEs and advertises them to the CE; the other VRF receives the routes advertised by the CE and advertises them to all PEs.

This command applies to IBGP or EBGP peers.

Configuration Examples

The following example allows the PE to receive messages with the same AS number as itself.

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.1.1.1 remote-as 100
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router-af)# neighbor 10.1.1.1 allowas-in
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.100 neighbor as-originate-interval

Use this command to configure the interval that the device advertises local original BGP routes to the peer (group). Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } as-origination-interval *seconds*

no neighbor { *peer-address* | *peer-group-name* } as-origination-interval

default neighbor { *peer-address* | *peer-group-name* } as-origination-interval

Parameter Description

Parameter	Description
<i>peer address</i>	IP address of the peer.
<i>peer-group-name</i>	Name of the peer group, containing up to 32 characters.
<i>seconds</i>	The interval at which the device advertises local original BGP routes to the peer (group), in the range from 1 to 65535 in the unit of seconds.

Defaults

The default interval is 1.

Command Mode

BGP configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP IPv6 VRF address family configuration mode/ BGP scope global configuration mode.

Usage Guide

If you specify a peer group name in this command, the configuration takes effect on all members of the peer group.

Configuration Examples

The following example configures the interval at which the device advertises local original BGP routes to the peer in the BGP IPv4 VRF address family configuration mode.

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router-af)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router-af)# neighbor 10.0.0.1 as-origination-interval 10
```

Related Commands

Command	Description
N/A	N/A

Platform

Description

N/A

5.101 neighbor as-override

Use this command to allow the PE to override the AS number of a site. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} as-override

no neighbor {*peer-address* | *peer-group-name*} as-override

default neighbor { *peer-address* | *peer-group-name* } as-override

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command

Mode BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope VRF configuration mode

In general, BGP will not receive the messages with the same AS number as the autonomous area. This command can override the AS number, so that BGP can receive the messages with the same AS number.

Usage

Guide

A typical application is in a VPN where two CEs have the same AS number. Usually the CEs cannot receive messages from each other. Executing this command on a PE will override the AS number of one CE it connects. As a result, the other CE can receive the peer's route messages. This command applies only to EBGp peers.

The following example allows the PE to override the AS number of a site.

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.1.1.1 remote-as 100
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router-af)# neighbor 10.1.1.1 as-override
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.102 neighbor default-originate

Use this command to allow the BGP speaker to advertise the default route to the peer (group). Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} default-originate [route-map *map-tag*]

no neighbor {*peer-address* | *peer-group-name*} default-originate [route-map *map-tag*]

default neighbor { *peer-address* | *peer-group-name* } default-originate [route-map *map-tag*]

Parameter	Description
<i>peer address</i>	IP address of the peer

<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>map-tag</i>	Name of the route-map of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, or BGP Scope configuration mode

Usage Guide This command requires redistributing the default route only when the default route exists locally. If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command. If you set the command for a member in the peer, this command will overwrite the settings on the peer group.

The following example allows the BGP speaker to advertise the default route to the peer (group).

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.1.1.1 remote-as 80
Ruijie(config-router)# neighbor 10.1.1.1 default-originate
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.103 neighbor description

Use this command to set a descriptive sentence for the specified peer (group). Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} description text

no neighbor {peer-address | peer-group-name} description

default neighbor { peer-address | peer-group-name } description

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>text</i>	Descriptive text of the peer (group) of up to 80 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode and BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage This command is used to add descriptive characters for the peer (group). This may help remember features and characteristics of the peer (group).

The following example sets a descriptive sentence for the specified peer (group).

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.1.1.1 remote-as 80
Ruijie(config-router)# neighbor 10.1.1.1 description xyz.com
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform
Description None

5.104 neighbor distribute-list

Use this command to implement the routing policy based on the ACL when receiving/sending route information from/to the specified BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **distribute-list** { *access-list-number* } { **in** | **out** }

no neighbor { *peer-address* | *peer-group-name* } **distribute-list** { *access-list-number* } { **in** | **out** }

default neighbor { *peer-address* | *peer-group-name* } **distribute-list** { *access-list-number* | *access-list-name* } { **in** | **out** }

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>access-list-number</i>	ACL number
in	Specifies the ACL for filtering the incoming routes.
out	Specifies the ACL for filtering the outgoing routes.

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage For in rule or out rule, this command cannot be used together with the **neighbor prefix-list** command. Only one of them can take effect.

Guide If you have specified the BGP peer group, all members of the peer group will adopt the settings. If you set the **neighbor distribute-list** command for a member in the peer, this command will overwrite the settings on the peer group.

You can set different filtering policies in different address-family configuration modes to control routes.

The following example implements the routing policy based on the ACL when receiving/sending route information from/to the specified BGP peer.

Configuration

```
Ruijie(config)# router bgp 60
```

Examples

```
Ruijie(config-router)# neighbor 10.1.1.1 remote-as 80
```

```
Ruijie(config-router)# neighbor 10.1.1.1
```

```
distribute-list bgp-filter in
```

Related**Commands**

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip access-list	Creates a standard IP ACL or extended IP ACL.

Platform**Description**

None

5.105 neighbor ebgp-multihop

Use this command to allow establishing BGP connection between EBGP peers that are not directly connected. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*tth*]

no neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*tth*]

default neighbor { *peer-address* | *peer-group-name* } **ebgp-multihop** [*tth*]

Parameter**Description**

Parameter	Description
<i>peer address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>tth</i>	Maximum hops in the range 1 to 255

Defaults

The BGP connection is allowed between EBGP peers connected with each other directly by default.

If "ebgp-multihop" is followed by no parameter, the tth is 255.

Command**Mode**

BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage**Guide**

To prevent routing loop and dampening, non-default routes that can reach the peer must exist between EBGP peers between which the BGP connection can only be established via multiple hops.

If the BGP peer group is specified, all members of the peer group adopt the settings. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

The following example allows establishing BGP connection between EBGP peers that are not directly connected.

Configuration Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 65100
Ruijie(config-router)# neighbor 10.0.0.1 ebgp-multihop
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.106 neighbor fall-over bfd

Use this command to enable BFD correlation with BGP. Use the **no** form or **default** form of this command to disable BFD correlation with BGP.

neighbor { *peer-address* | *peer-group-name* } **fall-over bfd**

no neighbor { *peer-address* | *peer-group-name* } **fall-over bfd**

default neighbor { *peer-address* | *peer-group-name* } **fall-over bfd**

Parameter Description

Parameter	Description
<i>peer address</i>	IPv4 or IPv6 address of the peer.
<i>peer-group-name</i>	Name of the peer group, containing up to 32 characters.

Defaults

BFD correlation is disabled by default.

Command Mode

BGP configuration mode / IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode/ Scope configuration mode

Usage Guide

Before configuring BFD correlation, the BFD session parameters of the neighbor interface must be configured.

Configuration Examples

The following example enables BFD correlation to detect the forwarding path between local and the neighbor 172.16.0.2.

```
Ruijie(config)# router bgp 45000
Ruijie(config-router)# neighbor 172.16.0.2 remote-as 45001
Ruijie(config-router)# neighbor 172.16.0.2 fall-over bfd
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform	
Description	None

5.107 neighbor filter-list

Use this command to enable route filtering when sending/receiving routing information to/from BGP peers. Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **filter-list** *access-list-number* { **in** | **out** }

no neighbor { *peer-address* | *peer-group-name* } **filter-list** *access-list-number* { **in** | **out** }

default neighbor { *peer-address* | *peer-group-name* } **filter-list** *access-list-number* { **in** | **out** }

Parameter	Description
<i>peer address</i>	IP address of the peer, IPv4 address or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>access-list-number</i>	ACL number
in	Applies as-path list on the received routing information.
out	Applies as-path list on the distributed routing information.

Defaults The function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage Guide If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If the **neighbor filter-list** command is set for a member of the peer, the setting will overwrite the setting for the group.

You can set different filter policies in different address-family configuration modes to control routes.

Configuration Examples The following example enables route filtering when sending/receiving routing information to/from BGP peers.

```
Ruijie(config)# ip as-path access-list 1 deny _123_
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 65100
Ruijie(config-router)# neighbor 10.0.0.1 filter-list 1 out
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip as-path access-list	Creates an AS_PATH list.
match as-path	Matches the AS_PATH list.

Platform None

Description

5.108 neighbor local-as

Use this command to configure the local AS number for the BGP peer, which could be used as its Remote AS to connect with local router. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **local-as** *as-number* [**no-prepend** [**replace-as** [**dual-as**]]]

no neighbor {*peer-address* | *peer-group-name*} **local-as**

Parameter
Description

Parameter	Description
<i>peer address</i>	IP address of the peer, IPv4 address or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>as-number</i>	Local AS number, in the range from 1 to 65535. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.
no-prepend	The AS-PATH of the routing information received from the peer does not depend on the Local AS. This option is disabled by default.
replace-as	The AS-PATH of the routing information sent to the peer replaces the BGP AS with the Local AS. This option is disabled by default.
dual-as	Uses BGP AS or Local AS to establish BGP connection with the device. This option is disabled by default.

Defaults

No Local AS is configured for the peer. If Local AS is configured, no option is configured by default. The peer could only use Local AS to establish BGP connection with local device, and adds Local AS into the AS-PATH of the received routing information, inserts Local AS to the corresponding AS-PATH before sending the routing information to the peer.

Command
Mode

BGP configuration mode, BGP IPv4/IPv6 VRF configuration mode or BGP Scope configuration mode.

Usage
Guide

Local AS could be configured on the EBGp peer only, and if the attributes of the peer change, such as EBGp converts to IBGP or union EBGp, Local AS and corresponding options will be deleted. Local AS must be different from BGP AS and this peer's Remote AS and the union ID (if federation is configured). If you have specified the BGP peer group, all members of this peer group will adopt the settings of this command. You cannot set Local AS for the specified member of the peer group separately.

Configuration
Examples

The following example configures the local AS number for the BGP peer.

```
Ruijie(config)# router bgp 65000
```

```
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 65100
Ruijie(config-router)# neighbor 10.0.0.1 local-as 23
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform

Description N/A

5.109 neighbor maximum-prefix

Use this command to limit the number of prefixes received from the specified BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

no neighbor {*peer-address* | *peer-group-name*} **maximum-prefix** *maximum*

default neighbor { *peer-address* | *peer-group-name* } **maximum-prefix** *maximum*

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>maximum</i>	Upper limit of the number of the received route entries
<i>threshold</i>	Percentage of the maximum when alarming.
warning-only	Does not terminate the BGP connection when the route entries reach the upper limit but produce a log entry.

Defaults This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide

The BGP connection will be torn down when the received routes exceeds the upper limit by default. To prevent tearing down the connection, set the "warning-only" to control that. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples

The following example limits the number of prefixes received from the specified BGP peer.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 maximum-prefix 1000
```

Related

Command	Description
---------	-------------

Commands	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.110 neighbor next-hop-self

Use this command to set the next-hop of the route to the local BGP speaker while specifying the routes that the BGP peer redistributes. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

no neighbor {*peer-address* | *peer-group-name*} **next-hop-self**

default neighbor { *peer-address* | *peer-group-name* } **next-hop-self**

	Parameter	Description
Parameter Description	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

Usage This command is mostly used in the non-full-mesh-type network, such as the Frame Relay and X.25, where the BGP speakers within the same subnet cannot completely be accessed mutually.

Guide If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command.

Configuration Examples The following example sets the next-hop of the route to the local BGP speaker.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 next-hop-self
```

	Command	Description
Related Commands	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.111 neighbor next-hop-unchanged

Use this command to maintain the next-hop when sending routes to the peer(group). Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **next-hop-unchanged**

no neighbor {*peer-address* | *peer-group-name*} **next-hop-unchanged**

default neighbor { *peer-address* | *peer-group-name* } **next-hop-unchanged**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
next-hop-unchanged	Maintains the next-hop while sending the routes to the peer(group).

Defaults

The next-hop will be changed by default when routes are sent to the EBGp peer.

Command Mode

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPLS/VPWS/EVPN address family configuration mode or BGP Scope Global configuration mode.

Usage Guide

This command is used to control to maintain the next-hop route transmitting between multi-hop EBGp peer sessions. This command cannot be configured on the route reflector. And for the client of the route reflector, if this function is enabled, the **neighbor next-hop-self** command cannot be used to change the next-hop of routes. This function is mainly applied to the cross-domain VPN. In the implementation with the Option C adopted, to reduce the complete connectivity between the PEs of the cross-domain CPN, a route reflector can be set in every autonomous domain to establish the Multihop MP-EBGP connection to implement the VPN route interaction. As the next-hop route is changed as itself while sending routes to the EBGp peer by default, PE stations of other autonomous domains will consider the final next-hop of the VPN route as the route reflector when receiving the VPN route at last, which will result in all cross-domains VPN flow going through the reflector. However, usually this is not the optimal forwarding path, and the requirement for the forwarding performance of the RR is higher. To avoid this condition, use the **neighbor next-hop-unchanged** command in the address-family VPNv4 configuration mode to maintain the next-hop of the VPNv4 route sent to the BGP peer when establishing the cross-domain Multihop MP-EBGP connection on the router reflector.

Configuration Examples

The following example maintains the next-hop when sending routes to the peer (group).

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# address-family vpnv4
Ruijie(config-router-af)# neighbor 10.1.1.1 next-hop-unchanged
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

neighbor remote-as	Configures the BGP peer.
---------------------------	--------------------------

Platform**Description** None

5.112 neighbor password

When the BGP connection with the BGP peer is established, use this command to enable TCP MD5 authentication and set the password. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **password** [0 | 7]*string*

no neighbor {*peer-address* | *peer-group-name*} **password**

default neighbor { *peer-address* | *peer-group-name* } **password**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
0	Displays the password with encryption.
7	Displays the password without encryption.
<i>string</i>	Password for MD5 authentication in the range from up to 80 characters

Defaults The function is disabled by default**Command Mode** BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.**Usage Guide**

This command will enable MD5 authentication of the TCP. BGP peers must have the same password configured; otherwise, the neighbor relationship cannot be established. When this command is set, the local BGP speaker will re-establish the BGP connection with the BGP peer. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

No matter in which mode, a neighbor has only one password, not one for every address family, .

Configuration Examples

The following example enables TCP MD5 authentication and sets the password.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 password Red-Giant
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol
neighbor remote-as	Configures the BGP peer.

Platform	
Description	None

5.113 neighbor peer-group (assigning members)

Use this command to configure the specified peer as a member of the BGP peer group. Use the **no** or **default** form of this command to restore the default setting.

neighbor *peer-address* **peer-group** *peer-group-name*

no neighbor *peer-address* **peer-group** *peer-group-name*


default neighbor *peer-address* **peer-group** *peer-group-name*

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults No peer exists in the peer group.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide Members of the peer group can adopt all configurations of the peer. It is allowed to configure an individual member of the peer group to replace the universal configuration for the peer group, but such separate configuration does not contain the configuration information that may affect the output update. In other words, every member in the peer group will always adopt the following configurations of the peer group:
remote-as, update-source, local-as, reconnect-interval, times, advertisement-interval, default-originate, next-hop-self, remove-private-as, send-community, distribute-list out, filter-list out, prefix-list out, route-map out, unsuppress-map, route-reflector-client.

 Do not place neighbors of different address families in the same peer group, or place IBGP and EBGP neighbors in the same peer group.

Configuration Examples The following example configures the specified peer as a member of the BGP peer group.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor Red-Giant peer-group
Ruijie(config-router)# neighbor 10.0.0.1 peer-group Red-Giant
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
neighbor peer-group (creating)	Creates the BGP peer group.

show ip bgp peer-group	Displays the information of the BGP peer.
-----------------------------------	---

Platform**Description** None

5.114 neighbor peer-group (creating)

Use this command to create a BGP peer group. Use the **no** or **default** form of this command to restore the default setting.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

default neighbor *peer-group-name* **peer-group**

Parameter	Parameter	Description
Description	<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults No BGP peer group is created.**Command Mode** BGP configuration mode, BGP IPv4/IPv6 VRF configuration mode or BGP Scope configuration mode.**Usage Guide** If multiple BGP peers use the same update policy, the peers can be configured in the same peer group, so as to simplify the configuration and boost operation efficiency.**Configuration Examples** The following example creates a BGP peer group.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor Red-Giant peer-group
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
neighbor peer-group (assigning members)	Configures the specified peer as the member of the BGP peer group.
show ip bgp peer-group	Displays the information of the BGP peer.

Platform**Description** None

5.115 neighbor prefix-list

Use this command to implement the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {in | out}

no neighbor {*peer-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {in | out}

default neighbor { *peer-address* | *peer-group-name* } **prefix-list** *prefix-list-name* { in | out }

Parameter	Description
<i>peer address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>prefix-lis-name</i>	Name of the prefix-list of up to 32 characters
in	Applies the prefix list to the received routes.
out	Applies the prefix list to the redistributed routes.

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.

For the "in" rule or "out" rule, this command cannot be used together with the **neighbor distribute-list** command. That is, only one of them takes effect.

Usage Guide If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If the **neighbor prefix-list in** command is set for a member of the peer, the setting will overwrite the setting for the group.

You can set different filter policies in different address-family configuration modes to control routes.

Configuration Examples The following example implements the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer.

```
Ruijie(config)# ip prefix-list bgp-filter deny 10.0.0.1/16
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 prefix-list bgp-filter in
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip prefix-list	Creates the prefix lists.

Platform Description None

5.116 neighbor remote-as

Use this command to configure the BGP peer (group). Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } remote-as *as-number*

no neighbor { *peer-address* | *peer-group-name* } remote-as

default neighbor { *peer-address* | *peer-group-name* } remote-as

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>as-number</i>	BGP peer (group) autonomous system number in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.

Defaults No BGP peer is configured.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.

Configuration Examples The following example configures the BGP peer (group).

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 80
```

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.

Platform Description None

5.117 neighbor remove-private-as

Use this command to delete the private AS number recorded in the AS path attribute in the route sent to the specified EBGW peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} remove-private-as

no neighbor {*peer-address* | *peer-group-name*} remove-private-as

default neighbor { *peer-address* | *peer-group-name* } remove-private-as

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, or BGP IPv4 VRF configuration mode.

This command takes effect only on EBGp peers.

Usage Guide If the AS path contains the private AS number that is the AS number of the EBGp peer to be sent, the AS number is not deleted.

Private AS number range: 64512 - 65535

Configuration Examples The following example deletes the private AS number recorded in the AS path attribute in the route sent to the specified EBGp peer

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 remove-private-as
```

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description None

5.118 neighbor route-map

Use this command to enable route match for the received/sent routes. Use the **no** or **default** form of this command to disable this function.

neighbor { *peer-address* | *peer-group-name* } route-map *map-tag* {in | out}

no neighbor { *peer-address* | *peer-group-name* } route-map *map-tag* {in | out}

default neighbor { *peer-address* | *peer-group-name* } route-map *map-tag* { in | out }

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>map-tag</i>	Name of the match rule
in	Applies the rule to the incoming routes.

out	Applies the rule to the outgoing routes.
------------	--

Defaults N/A

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.

Usage Guide This command can be used to filter the incoming and outgoing routes for different neighbors by using different incoming/outgoing rules, purifying and controlling routes.
You can set different filter policies in different address-family configuration modes to control routes.

Configuration Examples The following example enables route match for the received/sent routes.

```
Ruijie(config-router)# neighbor 10.0.0.1 route-map map-tag in
```

Related Commands

Command	Description
neighbor soft-reconfiguration inbound	Stores the routing information sent from the BGP peer.
show ip bgp	Displays the BGP route entry.

Platform

Description None

5.119 neighbor route-reflector-client

Use this command to configure the local device as the route reflector and specifies its client. Use the **no** or **default** form of this command to restore the default setting.

neighbor *peer-address* **route-reflector-client**

no neighbor *peer-address* **route-reflector-client**

default neighbor { *peer-address* | *peer-group-name* } **route-reflector-client**

Parameter

Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer. The name cannot exceed 32 characters.

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6/L2VPN VPWS/VPLS/EVPN address family configuration mode or BGP Scope configuration mode.

Usage By default, all IBGP speakers in the autonomous system must establish neighbor relationship with

Guide each other. The BGP speaker does not forward the routes learned from an IBGP peer to other IBGP peers to avoid route loop.

This command can be used to set route reflector, so that there is no need for all IBGP speakers to establish full neighboring relationship between each other. This will allow the route reflector to forward learned IBGP routes to other IBGP peers.

Configuration Examples

The following example configures the local device as the route reflector and specifies its client.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 route-reflector-client
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
bgp cluster-id	Configures the cluster ID of the route reflectors.
bgp client-to-client reflection	Enables the route reflection between clients

Platform

Description None

5.120 neighbor send-community

Use this command to transmit community attributes to the specified BGP neighbor. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
no neighbor {*peer-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
default neighbor { *peer-address* | *peer-group-name* } **send-community** [**both** | **standard** | **extended**]

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
both	Transmits both standard and extended communities.
standard	Transmits the standard community only.
extended	Transmits the extended community only.

Defaults This function is disabled by default.

Command Mode

BGP configuration mode, BGP IPv4 Unicast VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP L2VPN VPWS/VPLS address family configuration mode, BGP scope configuration mode

Usage

Guide This command transmits the community to the neighbor or neighbor group.

Configuration The following example transmits community attributes to the specified BGP neighbor.

Examples

```
Ruijie(config-router)# neighbor 10.1.1.1 send-community both
```

**Related
Commands**

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip community-list	Creates the community list.

Platform

Description None

5.121 neighbor send-label

Use this command to specify the device to send the route carrying the MPLS label to a neighbor. Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} send-label

no neighbor {peer-address | peer-group-name} send-label

default neighbor { peer-address | peer-group-name } send-label

**Parameter
Description**

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

**Command
Mode** BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

**Usage
Guide**

Use this command to allow the BGP sending the routes with MPLS label requiring two ends of the peer should be configured this command. The configuration of this command takes effect only after the neighbor is restarted. This command is configured in BGP configuration mode and takes effect on the ipv4 unicast address-family only by default. For AS border routers, only when this command is configured, the MPLS label can be forwarded on the AS border.

**Configuration
Examples**

The following example specifies the device to send the route carrying the MPLS label to a neighbor.

```
Ruijie(config)# router bgp 100
Ruijie(config-router)# neighbor 192.168.0.1 remote-as 101
Ruijie(config-router)# neighbor 192.168.0.1 send-label
```

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.

Platform**Description** N/A

5.122 neighbor shutdown

Use this command to disconnect the BGP connection established with the specified BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} shutdown

no neighbor {peer-address | peer-group-name} shutdown

default neighbor { peer-address | peer-group-name } shutdown

Use this command to gracefully disconnect the BGP connection established with the specified BGP peer.

neighbor { peer-address | peer-group-name } shutdown graceful [community value] [delay time]

Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	graceful	Shuts down BGP connection gracefully.
	community value	Indicates the community value carried in the route sent to the neighbor.
	delay time	Indicates the delay time (in seconds) for shutting down BGP connections. The value range is from 1 to 65,535.

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage This command is used to disconnect valid connection established with the specified peer (group), and delete all associated routing information. However, this command still keeps the configuration information of that specified peer (group).

Guide If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples The following example disconnects the BGP connection established with the specified BGP peer.

```
Ruijie(config)# router bgp 60
```

```
Ruijie(config-router)# neighbor 10.0.0.1 shutdown
```

	Command	Description
Related Commands	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	show ip bgp summary	Displays the BGP connection status.

Platform**Description** None

5.123 neighbor soft-reconfiguration inbound

Use this command to store the routing information sent from the BGP peer. Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} soft-reconfiguration inbound

no neighbor {peer-address | peer-group-name} soft-reconfiguration inbound

default neighbor { peer-address | peer-group-name } soft-reconfiguration inbound

	Parameter	Description
Parameter Description	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4 Unicast VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP L2VPN VPWS/VPLS address family configuration mode, BGP scope configuration mode

This command restarts the BGP session, and keeps the unchanged routing information sent from the BGP peer (group).

Usage Guide Executing this command will consume more memories. If both parties support the route refresh function, this command becomes unnecessary. You may run the **show ip bgp neighbors** command to judge whether the peer can support the route refresh function.

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration Examples The following example stores the routing information sent from the BGP peer.

```
Ruijie(config)# router bgp 65000
```

```
Ruijie(config-router)# neighbor 10.0.0.1 soft-reconfiguration inbound
```

	Command	Description
--	---------	-------------

Commands	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	show ip bgp neighbors	Displays the information of the BGP peer.
	clear ip bgp	Resets the BGP peer session.

Platform**Description** None

5.124 neighbor soo

Use this command to set the SOO value of the neighbor. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **soo** *soo-value*

no neighbor {*peer-address* | *peer-group-name*} **soo**

default neighbor { *peer-address* | *peer-group-name* } **soo**

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
Parameter Description <i>soo-value</i>	SOO value There are two forms of soo_value: (1)soo_value = as_num:nn as_number:nn: as_number is the public AS number and nn is defined by yourself. The range is from 0 to 4294967295. (2)soo_value = ip_addr:nn ip_address:nn: IP address must be global and nn is defined by yourself. The range is from 0 to 65535. (3)soo_value = as4_num:nn as4_num is the public AS number (4 byte) and nn is defined by yourself, which ranges from 0 to 65535.

Defaults This function is disabled by default.**Command****Mode** BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope VRF configuration mode.**Usage Guide** In CE dual-home mode, execute this command to prevent routes sent by CE to PEs from being sent back to CE.**Configuration**

The following example sets the SOO value of the neighbor.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
```

```
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router)# neighbor 10.0.0.1 soo 100:100
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
timers bgp	Configures the keepalive and holdtime values globally.

Platform

Description None

5.125 neighbor timers

In specifying BGP peer to establish the BGP connection, use this command to set the keepalive and holdtime time values used for establishing the BGP connection. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **timers** *keepalive holdtime* [*minimum-holdtime*]

no neighbor [*peer-address* | *peer-group-name*] **timers**

default neighbor { *peer-address* | *peer-group-name* } **timers** [**connect**]

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>keepalive</i>	Time interval to send the KEEPALIVE message to the BGP peer. Range: 0-65535 seconds
<i>holdtime</i>	Time interval to consider the BGP peer alive Range: 0-65535 seconds
<i>minimum-holdtime</i>	Allows a minimum holdtime value of neighbor advertisement. It is unrestricted when the value is 0. The range is 0 to 65535 seconds.
<i>connect-retry</i>	The value of the connect-retry timer is 15s.

Defaults

keepalive: 60 seconds
holdtime: 180 seconds
minimum-holdtime: 0 seconds
connect-retry: 15 seconds

Command Mode

BGP configuration mode, BGP IPv4 VRF address family configuration mode, BGP IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide

A proper keepalive value must not exceed one-third of the holdtime value.

If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer.

If the BGP peer group is specified, all members of the peer group adopt the settings of this

command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

The following example sets the keepalive and holdtime time values used for establishing the BGP connection.

Configuration**Examples**

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 80 240
```

The following example sets the connect-retry time values used for establishing the BGP connection.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 timers connect 100
```

**Related
Commands**

Command	Description
router bgp	Enables the BGP protocol.
timers bgp	Sets the keepalive and holdtime values globally.

Platform

Description None

5.126 neighbor unsuppress-map

Use this command to selectively advertise routing information suppressed by aggregate-address command. Use the **no** or **default** form of this command to restore the default setting.

neighbor {peer-address | peer-group-name} unsuppress-map map-tag

no neighbor {peer-address | peer-group-name} unsuppress-map map-tag

default neighbor { peer-address | peer-group-name } unsuppress-map map-tag

Parameter**Description**

Parameter	Description
<i>peer-address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>map-tag</i>	Name of the route-map of up to 32 characters

Defaults

This function is disabled by default.

Command**Mode**

BGP configuration mode, BGP IPv4 Unicast/VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP L2VPN VPWS/VPLS address family configuration mode, BGP scope configuration mode

Usage

This command advertises the specified suppressed routes.

Guide

If the BGP peer group is specified, all members of the peer group adopt the settings of this

command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

The following example selectively advertises routing information suppressed by aggregate-address command.

Configuration Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 unsuppress-map
unspress-route
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
aggregate-address	Configures the aggregate address.
route-map	Configures the route-map

Platform

Description None

5.127 neighbor update-source

Use this command to configure the interface for BGP connection of the IBGP peer..

neighbor { peer-address | peer-group-name } **update-source** {interface-type interface-number | address }

Use the **no** form of the command to remove the source address configuration for the BGP peer.

no neighbor {peer-address | peer-group-name} **update-source**

Use the **default** form of the command to restore the default settings.

default neighbor { peer-address | peer-group-name } **update-source**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>interface-type</i> <i>interface-number</i>	Interface name
<i>address</i>	The interface address which is used for BGP connection. The address type (IPv4 or IPv6) must be same as that of the peer address.

Defaults

The local interface is used as the egress interface by default.

Command

BGP configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family

Mode configuration mode/ Scope configuration mode

You can use this command to enable the loopback interface to establish a BGP connection with the peer.

The interface address specified for BGP connection must be valid in local, otherwise the BGP connection may be faulty.

All members in a BGP peer group inherit the settings of this command. Particularly, if the interface address is used, only the member whose address type is same as the interface address's can inherit the settings of this command.

Usage

Guide

If the IPv6 address of the loopback interface is used for neighbor connection, both peers need to be configured with the loopback interface. The BGP connection can be established only when the address of the egress interface on the peer is same as that of the neighbor in local.

A loopback interface address can be configured on different interfaces. You need to specify only the interface name,

The peer configured with the IPv6 address of loopback interface support only one-hop BGP neighbor connection.

Configuration Examples

The following example establishes the BGP connection.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 update-source loopback 1
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.128 neighbor version

Use this command to display the number of the BGP protocol version used by the specific BGP neighbor. Use the **no** or **default** form of this command to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **version** *number*

no neighbor { *peer-address* | *peer-group-name* } **version**

default neighbor { *peer-address* | *peer-group-name* } **version**

Parameter

Description

Parameter	Description
<i>peer-address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>number</i>	Version number

Defaults

The default version number is 4.

Command Mode BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode

Usage

Guide When the command is used, BGP will lose the version negotiation function.

Configuration Examples

The following example displays the number of the BGP protocol version used by the specific BGP neighbor.

```
Ruijie(config-router)# neighbor 10.1.1.1 version 4
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.129 neighbor weight

Use this command to set the weight for the specific neighbor. Use the **no** or **default** form of this command to restore the default setting.

neighbor {*peer-address*|*peer-group-name*} **weight** *number*

no neighbor {*peer-address*|*peer-group-name*} **weight**

default neighbor { *peer-address* | *peer-group-name* } **weight**

Parameter Description

Parameter	Description
<i>peer-address</i>	IP address of the peer
<i>peer-group-name</i>	Name of the peer group of up to 32 characters
<i>number</i>	Weight, in the range from 0 to 65535.

Defaults

No weight is configured for the specific neighbor by default. In this case, the learned route weight is 0 and the locally generated route's weight is 32768 initially.

Command Mode

BGP configuration mode, BGP IPv4 Unicast/VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP L2VPN VPWS/VPLS address family configuration mode, BGP scope configuration mode

Usage

When the command is used, routes learnt from the neighbor use this value as the initial weight value. The higher the weight, the higher the priority is.

Guide

Executing the **set weight** command in the route map of the neighbor will overwrite this value.

Configuration

The following example sets the weight for the specific neighbor.

Examples

```
Ruijie(config-router)# neighbor 10.1.1.1 weight 73
```

**Related
Commands**

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform

Description None

5.130 network

Use this command to configure the network information to be advertised by the local BGP speaker. Use the **no** or **default** form of this command to restore the default setting.

network *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]

no network *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]

default network *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]

**Parameter
Description**

Parameter	Description
<i>network-number</i>	Network number
<i>mask</i>	Subnet mask
<i>map-tag</i>	Name of the route-map of up to 32 characters
backdoor	The route is a backdoor route.

Defaults

No network information is specified by default.

**Command
Mode**

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

**Usage
Guide**

This command allows injecting the IGP route into the BGP routing table. The network information advertised can be direct route, static route and dynamic route.

The "route-map" can be used to modify the network information.

**Configuration
Examples**

The following example configures the network information to be advertised by the local BGP speaker.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# network 10.0.0.1 mask 255.255.0.0
```

**Related
Commands**

Command	Description
router bgp	Enables the BGP protocol.
redistribute	Configures the route redistribution.
Network synchronization	Enables network synchronization.

Platform	
Description	None

5.131 network synchronization

Use this command to advertise the network information after the local BGP speaker is synchronized with the local device. Use the **no** or **default** form of this command to directly advertise the network information.

network synchronization

no network synchronization

default network synchronization

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide This command is used to modify the status of the network during the process of advertisement. It is not recommended to turn off this switch lest route black hole is caused.

Configuration Examples The following example advertises the network information after the local BGP speaker is synchronized with the local device.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# network synchronization
```

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	redistribute	Configures the route redistribution.
	network(BGP)	Configures the route to be distributed.

Platform	
Description	None

5.132 overflow memory-lack

Use this command to allow BGP to enter the OVERFLOW state when the memory is insufficient. Use the **no** or **default** form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

default overflow memory-lack

Parameter
Description

Parameter	Description
N/A	N/A

Defaults

Allow the BGP to enter the OVERFLOW state when the memory is insufficient.

Command

Mode

BGP configuration mode or BGP Scope Global configuration mode

In the BGP OVERFLOW state, the newly-learned routes are discarded, which prevents the memory from increasing.

When this function is enabled, if the BGP address family is in the OVERFLOW state, the newly-learned routes will be discarded, which may result in network loop. To prevent this, BGP generates a default route directing to the NULL interface, and the default route will always exist in the OVERFLOW state.

Usage

Guide

Use the **clear bgp {addressfamily|all} *** command to reset the BGP and clear the OVERFLOW state in the BGP address family.

Use the no option to disallow the BGP to enter the OVERFLOW state when the memory is insufficient, which may lead to the continuous exhaustion of the memory resources. When the memory has been exhausted to a certain degree, BGP will break down all neighbors and delete all learned routes.

Configuration

The following example sets BGP not to enter the OVERFLOW configuration status when the memory is insufficient.

Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# no overflow memory-lack
```

Related

Commands

Command	Description
clear bgp { addressfamily all } *	Resets the BGP address family.
show bgp { addressfamily all } summary	Displays the summary of the BGP address family.

Platform

Description

None

5.133 redistribute

Use this to redistribute routes between the other routing protocol and the BGP. Use the **no** or **default** form of this command to restore the default setting.

redistribute protocol-type [route-map map-tag] [metric metric-value]

no redistribute protocol-type [route-map map-tag] [metric]

default redistribute protocol-type [route-map *map-tag*] [metric]

Parameter	Description
<i>protocol-type</i>	The source protocol types for redistributing routes, including connected, static, RIP
route-map <i>map-tag</i>	Specifies the route map. No route map is associated with by default.
metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by default.

**Parameter
Description**

Defaults



This function is disabled by default.

**Command
Mode**

BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol. This is applicable to all IP routing protocols.

**Usage
Guide**

-  When you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The no form removes redistribution without any parameters configured.
-  The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are unavailable, the redistributed one is used.

**Configuration
Examples**

The following example redistributes routes between the other routing protocol and the BGP.

```
Ruijie(config-router)# redistribute static route-map static-rmap
Ruijie(config-router)# no redistribute static
route-map static-rmap
Ruijie(config-router)# no redistribute static
```

**Related
Commands**

Command	Description
show ip protocol	Displays the protocol configuration.

Platform

Description None

5.134 redistribute isis

Use this command to redistribute routes between ISIS and BGP. Use the **no** or **default** form of this command to restore the default setting.

redistribute isis [isis-tag] [route-map *map-tag*] [metric *metric-value*] [level-1 | level-1-2 | level-2]

no redistribute isis [*isis-tag*] [**route-map** *map-tag*] [**metric**] [**level-1** | **level-1-2** | **level-2**]

default redistribute isis [*isis-tag*] [**route-map** *map-tag*] [**metric**] [**level-1** | **level-1-2** | **level-2**]

**Parameter
Description**



Parameter	Description
<i>isis-tag</i>	(Optional)ISIS process ID to be redistributed
route-map <i>map-tag</i>	Specifies the route map. No route map is associated by default.
metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by default.
level-1	Redistributes level-1 ISIS routes.
level-1-2	Redistributes level-1 and level-2 ISIS routes.
level-2	Redistributes level-2 ISIS routes.

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol. This is applicable to all IP routing protocols.

**Usage
Guide**

-  When you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.
-  The filtering rule of ISIS routing is: filtering the ISIS routing type according to the configured level option before filtering the route-map rule. The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are unavailable, the redistributed one is used.

**Configuration
Examples**

The following example redistributes routes between ISIS and BGP.

```
Ruijie(config-router)# redistribute isis route-map static-rmap
Ruijie(config-router)# no redistribute isis test route-map isis-rmap
Ruijie(config-router)# no redistribute isis
```

**Related
Commands**

Command	Description
show ip protocol	Displays the protocol configuration.

**Platform
Description**

None

5.135 redistribute ospf

Use this command to redistribute routes between OSPF and BGP. Use the **no** or **default** form of this command to restore the default setting.

redistribute ospf *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [1|2]] **nssa-external** [1|2]]

no redistribute ospf *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external** [1|2]] **nssa-external** [1|2]]

default redistribute ospf *process-id* [**route-map** *map-tag*] [**metric**] [**match** { **internal** | **external** [1 | 2] } | **nssa-external** [1 | 2] }

Parameter Description


Parameter	Description
<i>process-id</i>	OSPF process ID to be redistributed
route-map <i>map-tag</i>	Specifies the route map. No route map is associated by default.
metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by default.
match	Matches the sub type of OSPF routes.
internal	Matches the internal OSPF routes, the default configuration.
external [1 2]	Matches the external OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.
nssa-external [1 2]	Matches the NSSA-external type of OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.


Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol.

Usage Guide

 When you configure the **no** form of this command with parameters, the corresponding parameter configuration will be removed. The **no** form removes redistribution without any parameters configured.

 The filtering rule of OSPF routing: filtering the OSPF routing type according to the configured match option before filtering the route-map rule. The route metric generated by the **route-map** command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.

Configuration The following example redistributes routes between OSPF and BGP.

Examples

```
Ruijie(config-router)# redistribute ospf 2 route-map static-rmap
Ruijie(config-router)# no redistribute ospf 4 match external route-map
ospf-rmap
Ruijie(config-router)# no redistribute ospf 78
```

Related**Commands**

Command	Description
show ip protocol	Displays the protocol configuration.

Platform**Description**

None

5.136 router bgp

Use this command to enable the BGP protocol, configure the local autonomous system number and enter BGP protocol configuration mode. Use the **no** or **default** form of this command to restore the default setting.

router bgp *as-number*

no router bgp *as-number*

default router bgp *as-number*

**Parameter
Description**

Parameter	Description
<i>as-number</i>	AS number in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.

Defaults

This function is disabled by default.

Command**Mode**

Global configuration mode

**Usage
Guide**

This command is used to start the BGP protocol.

RFC4839 defines a new reserved AS notation 23456, which cannot be used. The original private AS notation in the range from 64512 to 65534 is still effective, 65535 is reserved for special purposes.

RFC 5398 also defines two groups of new reserved AS notation for documents, whose ranges are from 64496 to 64511 and from 65536 to 65551.

Configuration

The following example enables the BGP protocol.

Examples

```
Ruijie(config)# router bgp 65000
```

Related**Commands**

Command	Description
ip routing	Enables IP routing.

bgp router-id	Sets the ID of the device running the BGP protocol
network	Sets the network information to be advertised by the local BGP speaker.

Platform**Description** None

5.137 scope

Use this command to enter the scope configuration mode and associate VRF with BGP. Use the **exit** command to exit the scope configuration mode. Use the **no** or **default** form of this command to remove the association between the VRF instance and BGP protocol.

scope { **global** | **vrf** *vrf-name* }

exit

no scope { **global** | **vrf** *vrf-name* }

default scope { **global** | **vrf** *vrf-name* }


Parameter	Description
global	Global routing table.
vrf <i>vrf-name</i>	VRF name.

Defaults No scope address family is defined by default.**Command****Mode** BGP configuration mode.

Enter the scope configuration mode to perform the configuration.

To exit the scope configuration mode, use the **exit** command.

Usage**Guide**

 In the scope configuration mode, the commands configured in the BGP configuration mode are converted to the form in the scope configuration mode. To restore the commands, execute the command **no route bgp** and configure the commands again.

Configuration**Examples**

The following example enters the scope global configuration mode.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# scope global
```

Related**Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

5.138 show bgp all

Use this command to display all the address-families information of BGP route. The use of this command is consistent with other BGP's show commands.

Display the parameters of the route information.

```
show bgp all [ community [ community-number [ exact-match ] ] | filter-list path-list-number |
community-list community-name [ exact-match ] | extcommunity-list extcommunity-name | regexp
regexp | quote-regexp regexp | inconsistent-as ]
```

Display the route dampening parameter.

```
show bgp all dampening { flap-statistics | dampened-paths | parameters }
```

Display the related information of the neighbors.

```
show bgp all neighbors [ peer-address [ received-routes | routes | advertised-routes | policy
[ detail ] ] ]
```

```
show bgp all summary
```

Display the path information.

```
show bgp all paths
```

Parameter
Description

Parameter	Description
community <i>community-number</i>	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
community-list <i>community-name</i>	Displays the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matching the community value or community-list.
dampening dampened-paths	Displays the restrained routing information.
dampening flap-statistics	Displays the routing dampening statistics.
dampening parameters	Displays the routing dampening parameters.
extcommunity-list <i>extcommunity-name</i>	Displays the routing information including the specified extcommunity value.
filter-list <i>path-list-number</i>	Displays the routing information matching the filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.

neighbors [<i>peer-address</i>]	Displays all the BGP neighbors' information.
neighbors <i>peer-address</i> received-route	Displays all routing information received from the specified peer (including the accepted and refused route).
neighbors <i>peer-address</i> routes	Displays all the accepted routing information received from the peer.
neighbors <i>peer-address</i> advertised-routes	Displays all the routing information sent to the specified peer.
neighbors <i>peer-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>peer-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
quote-regexp <i>regex</i>	Displays the BGP routing information with the AS path attribute matching the specified regex within the double quote marks.
regexp <i>regex</i>	Displays the BGP routing information with the AS path attribute matching the specified regex.

Defaults Please refer to the detailed description of **show bgp ipv4 unicast** command.

Command

Mode Privileged EXEC mode

Usage

Guide N/A

The following example shows all neighbors' information.

```
Ruijie(config)# show bgp all
For address family: IPv4 Unicast
BGP table version is 1, local router ID is 1.2.3.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric      LocPrf      Weight Path
*> 1.0.0.0          0.0.0.0           0           32768      ?

Total number of prefixes 1
```

Configuration

Examples


```

For address family: IPv6 Unicast

BGP table version is 1, local router ID is 1.2.3.4

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric      LocPrf      Weight Path
*> 5750:1::/120    ::                0           32768      ?

Total number of prefixes 1

```

**Related
Commands**

Command	Description
show bgp ipv4 unicast	Displays the IPv4 unicast route information of BGP

Platform

Description None

5.139 show bgp ipv4 unicast

Use this command to display the IPv4 unicast route information of BGP.

show bgp ipv4 unicast [vrf *vrf-name*] [network [*network-mask*]]

show bgp ipv4 unicast [vrf *vrf-name*] community *community-number* [exact-match]

show bgp ipv4 unicast [vrf *vrf-name*] community-list *community-name* [exact-match]

show bgp ipv4 unicast [vrf *vrf-name*] extcommunity-list *extcommunity-name*

show bgp ipv4 unicast [vrf *vrf-name*] dampening dampened-paths

show bgp ipv4 unicast [vrf *vrf-name*] dampening flap-statistics

show bgp ipv4 unicast [vrf *vrf-name*] filter-list *path-list-number*

show bgp ipv4 unicast [vrf *vrf-name*] inconsistent-as

show bgp ipv4 unicast [vrf *vrf-name*] prefix-list *ip-prefix-list-name*

show bgp ipv4 unicast [vrf *vrf-name*] quote-regexp *regexp*

show bgp ipv4 unicast [vrf *vrf-name*] regexp *regexp*

show bgp ipv4 unicast [vrf *vrf-name*] **route-map** *map-tag*

show bgp ipv4 unicast [vrf *vrf-name*] **neighbors** [*neighbor-address* [**received-routes** | **routes** | **advertised-routes** | **policy** [**detail**]]]

show bgp ipv4 unicast [vrf *vrf-name*] **cidr-only**

show bgp ipv4 unicast [vrf *vrf-name*] **labels**

Parameter	Description
<i>vrf-name</i>	VRF name
<i>network</i>	Displays the specific routing information in the routing table
<i>network-mask</i>	Displays the routing information included in the specified network.
longer-prefixes	Displays the route map information.
community <i>community-number</i>	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
community-list <i>community-name</i>	Displays the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matching the community value or community-list.
extcommunity-list <i>extcommunity-name</i>	Displays the routing information including the specified extcommunity value.
dampening dampened-paths	Displays the restrained routing information.
dampening flap-statistics	Displays the routing dampening statistics.
filter-list <i>path-list-number</i>	Displays the routing information matching the filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.
prefix-list <i>ip-prefix-list-name</i>	Displays the routing information matching the specified prefix-list.
quote-regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp.
route-map <i>map-tag</i>	Displays the routing information matching the specified route-map filtering condition.
neighbors [<i>neighbor-address</i>]	Displays the BGP IPv4 unicast neighbor information.
neighbors <i>neighbor-address</i> received-routes	Displays all routing information received from the specified peer (including the accepted and refused route).
neighbors <i>neighbor-address</i> routes	Displays all the routing information received from the peer and accepted.
neighbors <i>neighbor-address</i> advertised-routes	Displays all the routing information sent to the specified peer.
neighbors <i>neighbor-address</i>	Displays the related routing policy information of BGP neighbors.

Parameter
Description

policy	(General)
neighbors <i>neighbor-address</i>	Displays the related routing policy information of BGP neighbors.
policy detail	(Detail)
cidr-only	Displays the routing information without the category.
labels	Displays the BGP-learned and BGP-sent routes with the MPLS label.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Use this command to view the IPv4 unicast route information of BGP. You can filter the information with the specified parameter to display the matching route information.

The following example displays the IPv4 unicast route information of BGP.

```
Ruijie# show bgp ipv4 unicast
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network      Next Hop      Metric  LocPrf  Path
*>i44.0.0.0    192.168.195.183  0    100    i
*>i64.12.0.0/16 192.168.195.183  0    100    i
*>i172.16.0.0/24 192.168.195.183  0    100    i
*>i202.201.0.0  192.168.195.183  0    100    i
*>i202.201.1.0  192.168.195.183  0    100    i
*>i202.201.2.0  192.168.195.183  0    100    i
*>i202.201.3.0  192.168.195.183  0    100    i
*>i202.201.18.0 192.168.195.183  0    100    i
Total number of prefixes 8
Ruijie# show bgp ipv4 unicast community 11:2222
111:12345
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network      Next Hop      Metric  LocPrf  Path
*>i202.201.0.0  192.168.195.183  0    100    i
*>i202.201.1.0  192.168.195.183  0    100    i
*>i202.201.2.0  192.168.195.183  0    100    i
*>i202.201.3.0  192.168.195.183  0    100    i
Total number of prefixes 4
Ruijie(config)# ip as-path access-list 5 permit .*
```

Configuration Examples

```

Ruijie# show bgp ipv4 unicast filter-list 5
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      Next Hop      Metric  LocPrf  Path
*>192.168.88.0  0.0.0.0      32768  ?
Total number of prefixes 1
Ruijie# show ip bgp cidr-only
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      Next Hop      Metric  LocPrf  Path
*>i64.12.0.0/16 192.168.195.183 0    100    i
*>i172.16.0.0/24 192.168.195.183 0    100    i
Total number of prefixes 2
Ruijie# show bgp ipv4 unicast labels
Network      Next Hop      In Label/Out Label
1.1.1.1/32   192.167.1.1  17/18
1.1.1.2/32   192.167.1.1  no-label/19

```

Field	Description
Network	Route prefix
Nexthop	Nexthop IP address of the route
In label	Label assigned by this router (if any).
Out label	Label learnt from the nexthop router (if any).

**Related
Commands**

Command	Description
show ip bgp	Displays the IPv4 unicast route information of BGP.

Platform

Description None

5.140 show bgp ipv4 unicast dampening parameters

Use this command to display the IPv4 unicast route dampening parameters configured for the BGP.

show bgp ipv4 unicast [vrf *vrf-name*] dampening parameters

**Parameter
Description**

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults N/A

Command**Mode** Privileged EXEC mode**Usage** This command is used to display the IPv4 unicast route dampening parameters configured for BGP.
Guide

The following example displays the IPv4 unicast route dampening parameters configured for the BGP.

```
Ruijie(config-router)# bgp dampening 25 10000 10000 200
Ruijie# show bgp ipv4 unicast dampening parameters
dampening 25 10000 10000 200
Dampening Control Block(s):
Reachability Half-Life time : 25 min
Reuse penalty      : 10000
Suppress penalty   : 10000
Max suppress time  : 200 min
Max penalty (ceil) : 29800000
Min penalty (floor) : 5000
```

Configuration**Examples****Related****Commands** N/A**Platform****Description** None

5.141 show bgp ipv4 unicast neighbors

Use this command to display the related information of BGP IPv4 unicast neighbor.

show bgp ipv4 unicast [vrf *vrf-name*] neighbors *neighbor-address*

Parameter	Description
<i>vrf-name</i>	VRF name
<i>neighbor-address</i>	Neighbor IPv4 address
neighbors <i>neighbor-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>neighbor-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)

Defaults N/A**Command****Mode** Privileged EXEC mode

Usage**Guide**

This command is used to view the information of the connection with BGP IPv4 unicast neighbor.

The following example displays the related information of BGP IPv4 unicast neighbor.

```
Ruijie# show bgp ipv4 unicast neighbors
BGP neighbor is 192.168.195.183, remote AS 23, local AS 23, internal link
  BGP version 4, remote router ID 44.0.0.1
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
  Address family IPv4 Unicast: advertised and received
  Graceful restart: advertised and received
  Remote Restart timer is 120 seconds
  Received 14 messages, 0 notifications, 0 in queue
  open message:1 update message:4 keepalive message:9
  refresh message:0 dynamic cap:0 notifications:0
  Sent 12 messages, 0 notifications, 0 in queue
  open message:1 update message:3 keepalive message:8
  refresh message:0 dynamic cap:0 notifications:0
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds
  For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Inbound soft reconfiguration allowed
  8 accepted prefixes
  0 announced prefixes
  Connections established 2; dropped 1
  Local host: 192.168.195.239, Local port: 1074
  Foreign host: 192.168.195.183, Foreign port: 179
  Nexthop: 192.168.195.239
  Nexthop global: ::
  Nexthop local: ::
  BGP connection: non shared network
  Last Reset: 00:06:43, due to BGP Notification sent
  Notification Error Message: (Cease/Unspecified Error Subcode)
  Using BFD to detect fast fallover
```

**Configuration
Examples****Related****Commands**

N/A

Platform**Description**

None

5.142 show bgp ipv4 unicast paths

Use this command to display the path information of the IPv4 unicast in the route database.

show bgp ipv4 unicast [vrf *vrf-name*] paths

Parameter	Parameter	Description
Description	<i>vrf-name</i>	Indicates a specified VRF name.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

Guide This command is used to view the path information in the route database.

The following example displays the path information of the IPv4 unicast in the route database.

Configuration Examples

```
Ruijie# show bgp ipv4 unicast paths
Address Refcnt Path
[0x1d7806a0:0] (67)
[0x1d7389a0:13] (20) 10
```

Related

Commands N/A

Platform

Description None

5.143 show bgp ipv4 unicast summary

Use this command to display the related information of BGP IPv4 unicast.

show bgp ipv4 unicast [vrf *vrf-name*] summary

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

Guide This command is used to display the related information of BGP IPv4 unicast.

The following example displays the related information of BGP IPv4 unicast.

```
Ruijie # show bgp ipv4 unicast summary
BGP router identifier 192.168.183.1, local AS number 23
BGP table version is 2
2 BGP AS-PATH entries
1 BGP community entries
Neighbor  V AS MsgRcvd MsgSent TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.168.195.79 4 24   0   0   0 0 0 never Active
192.168.195.183 4 23  17  15   1 0 0 00:09:04  8
Total number of neighbors 2
```

Configuration Examples

Related Commands

Command	Description
router bgp	Enables the BGP protocol

Platform

Description None

5.144 show bgp ipv6 unicast

Use this command to display the IPv6 unicast routing information of BGP.

show bgp ipv6 unicast [vrf *vrf-name*] [*IPv6-Prefix*]

show bgp ipv6 unicast [vrf *vrf-name*]community *community-number* [exact-match]

show bgp ipv6 unicast [vrf *vrf-name*]community-list *community-name* [exact-match]

show bgp ipv6 unicast [vrf *vrf-name*] extcommunity-list *extcommunity-name*

show bgp ipv6 unicast [vrf *vrf-name*]dampening dampened-paths

show bgp ipv6 unicast [vrf *vrf-name*]dampening flap-statistics

show bgp ipv6 unicast [vrf *vrf-name*]filter-list *path-list-number*

show bgp ipv6 unicast [vrf *vrf-name*]inconsistent-as

show bgp ipv6 unicast [vrf *vrf-name*]prefix-list *ipv6-prefix-list-name*

show bgp ipv6 unicast [vrf *vrf-name*]quote-regexp *regexp*

show bgp ipv6 unicast [vrf *vrf-name*] regexp *regexp*

show bgp ipv6 unicast [vrf *vrf-name*] route-map *map-tag*

show bgp ipv6 unicast [vrf *vrf-name*]neighbors *neighbor-address*[received-routes | routes | advertised-routes]

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

<i>IPv6-prefix</i>	Displays the IPv6 routing information included in the specified network. The input format of the routing information prefix is X:X:X:X::X/<0-128>.
longer-prefixes	Displays the route map information.
community <i>community-number</i>	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
community-list <i>community-name</i>	Displays the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matches the community value or community-list.
extcommunity-list <i>extcommunity-name</i>	Displays the routing information including the specified extcommunity value.
dampening dampened-paths	Displays the restrained routing information.
dampening flap-statistics	Displays the routing dampening statistics.
filter-list <i>path-list-number</i>	Displays the routing information matching the filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.
prefix-list <i>ipv6-prefix-list-name</i>	Displays the routing information matching the specified prefix-list.
quote-regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp.
route-map <i>map-tag</i>	Displays the routing information matching the specified route-map filtering condition.
neighbors [<i>neighbor-address</i>]	Displays the BGP IPv6 unicast neighbor information.
neighbors <i>neighbor-address</i> received-routes	Displays all routing information received from the specified peer (including accepted and refused routes).
neighbors <i>neighbor-address</i> routes	Displays all the routing information received from the peer and accepted.
neighbors <i>neighbor-address</i> advertised-routes	Displays all the routing information sent to the specified peer.
neighbors <i>neighbor-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>neighbor-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide Use this command to view the IPv6 unicast route information of BGP. You can filter the information with the specified parameter to display the matching route information. The function and use of this command is similar to the **show bgp ipv4 unicast** command, please refer to the command.

Configuration

Examples N/A

Related Commands

Command	Description
show bgp ipv4 unicast	Displays the IPv4 unicast route information of BGP.

Platform

Description None

5.145 show bgp ipv6 unicast dampening parameters

Use this command to display the IPv6 unicast route dampening parameters configured for BGP.

show bgp ipv6 unicast [vrf *vrf-name*] dampening parameters

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide This command is used to display the IPv6 unicast route dampening parameters configured for the BGP. The function and use of this command are similar to the **show bgp ipv4 unicast dampening parameters** command. Please refer to the command.

Configuration

Examples N/A

Related Commands

Command	Description
show bgp ipv4 unicast dampening parameters	Displays the IPv4 unicast route dampening parameters configured for BGP.

Platform

Description None

5.146 show bgp ipv6 unicast neighbors

Use this command to display the related information of BGP IPv6 unicast neighbor.

show bgp ipv6 unicast [vrf *vrf-name*] neighbors *neighbor-address*

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name
	<i>neighbor-address</i>	Neighbor IPv6 address.
	neighbors <i>neighbor-address</i> policy	Related route policy information of BGP neighbor. (General)
	neighbors <i>neighbor-address</i> policy detail	Related route policy information of BGP neighbor. (Detail)

Defaults N/A

Command

Mode Privileged EXEC mode

Usage

This command is used to view the information of the connection with BGP IPv6 unicast neighbor.

Guide

The function and use of this command are similar to the **show bgp ipv4 unicast neighbors *neighbor-address*** command. Please refer to the command.

Configuration

Examples N/A

Related Commands	Command	Description
	show bgp ipv4 unicast neighbors <i>neighbor-address</i>	Displays the related information of BGP IPv4 unicast neighbor.

Platform

Description None

5.147 show bgp ipv6 unicast paths

Use this command to display the path information of the IPv6 unicast in the route database.

show bgp ipv6 unicast [vrf *vrf-name*] paths

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name

Defaults N/A

Command Privileged EXEC mode

Mode**Usage****Guide**

This command is used to view the path information in the route database.

The following example displays the path information of the IPv6 unicast in the route database.

Configuration**Examples**

```
Ruijie# show bgp ipv6 unicast paths
Address Refcnt Path
[0x1d7806a0:0] (67)
[0x1d7389a0:13] (20) 10
```

Related**Commands**

Command	Description
show bgp ipv4 unicast paths	Displays the path information of the IPv4 unicast in the route database.

Platform**Description**

None

5.148 show bgp ipv6 unicast summary

Use this command to display the related information of BGP IPv6 unicast.

show bgp ipv6 unicast [vrf *vrf-name*] summary

Parameter**Description**

Parameter	Description
vrf-name	VRF name.

Defaults

N/A

Command**Mode**

Privileged EXEC mode

Usage**Guide**

This command is used to display the related information of BGP IPv6 unicast. The function and use of this command are similar to the **show bgp ipv4 unicast summary** command. Please refer to the command.

Configuration**Examples**

N/A

Related**Commands**

Command	Description
router bgp	Enables the BGP protocol
show bgp ipv4 unicast summary	Displays the related information of BGP IPv4 unicast.

Platform

None

Description

5.149 show bgp l2vpn

Use the following command to display the BGP L2VPN routing information.

```
show bgp l2vpn { vpls | vpws | evpn } all
```

Use the following command to display the routing information of the BGP L2VPN address family of the *ve_id:offset*.

```
show bgp l2vpn { vpls | vpws } all ve_id:offset
```

Use the following command to display the neighbor information of the BGP L2VPN EVPN address family.

```
show bgp l2vpn evpn all { ethernet-ad | ethernet-segment | inclusive-multicast | ip-prefix | mac-ip } [ detail ]
```

Use the following command to display the neighbor information of the BGP L2VPN address family.

```
show bgp l2vpn { vpls | vpws | evpn } all neighbor [ peer-address [ policy [ detail ] ] ]
```

Use the following command to display the neighbor summary information of the BGP L2VPN address family.

```
show bgp l2vpn { vpls | vpws | evpn } all summary
```

Use the following command to display the L2VPN VPLS/VPWS information on the specified RD.

```
show bgp l2vpn { vpls | vpws } rd vpn_rd [ ve_id:offset ]
```

Use the following command to display the L2VPN VPLS/VPWS information on the specified VFI.

```
show bgp l2vpn { vpls | vpws } vfi vfi_name [ ve_id:offset ]
```

Use the following command to display the L2VPN EVPN information on the specified RD.

```
show bgp l2vpn evpn rd vpn_rd [[ethernet-ad | ethernet-segment | inclusive-multicast | ip-prefix | mac-ip ] [ detail ]]
```

Use the following command to display the L2VPN VPLS/VPWS information on the specified VFI.

```
show bgp l2vpn evpn evi vni-id [[ethernet-ad | ethernet-segment | inclusive-multicast | ip-prefix | mac-ip ] [ detail ]]
```

Parameter
Description

Parameter	Description
<i>vpls</i>	Displays VPLS information.
<i>vpws</i>	Displays VPWS information.
evpn	Displays EVPN information.
all	Displays all NLRI information that contains the VPLS instance or the VPWS instance.
<i>ve_id:offset</i>	Displays the VFI instance information of the specified

	ve_id:offset
ethernet-ad [detail]	Displays basic (detailed) information of the first type of BGP L2VPN EVPN routes.
ethernet-segment [detail]	Displays basic (detailed) information of the fourth type of BGP L2VPN EVPN routes.
inclusive-multicast [detail]	Displays basic (detailed) information of the third type of BGP L2VPN EVPN routes.
ip-prefix [detail]	Displays basic (detailed) information of the fifth type of BGP L2VPN EVPN routes.
ip-prefix [ip_addr [detail] ipv6_addr [detail] detail]	Displays basic (detailed) information of routes with specific IP address or IPv6 address in the fifth type of BGP L2VPN EVPN routes.
mac-ip [detail]	Displays basic (detailed) information of the second type of BGP L2VPN EVPN routes.
mac-ip mac_addr [ip_addr [detail] ipv6_addr [detail] detail]	Displays basic (detailed) information of routes with specific MAC addresses or MAC addresses+IP addresses/IPv6 addresses in the second type of BGP L2VPN EVPN routes.
neighbor [peer-address]	Displays the BGP L2VPN neighbor information. You can specify the specific neighbor information by entering the parameter <i>peer-address</i> . Otherwise all BGP L2VPN neighbor information is displayed.
neighbor peer-address policy	Displays the summarized routing policy information on BGP neighbor.
neighbor peer-address policy detail	Displays the detailed routing policy information BGP neighbor,
summary	Displays main BGP L2VPN information, including site ID, OFFSET, LABEL BASE and NEXT HOP.
rd vpn_rd	The specified RD.
vfi vfi_name	The specified VFI instance.
evi vni-id	The specified evl instance.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Use the command **show bgp l2vpn vpls** to display the VPLS information of local configuration, including Site ID, LABEL BASE and so on.

Configuration Examples

The following example displays all L2VPN VPLS address family routing information.

```
Ruijie(config)# show bgp l2vpn vpls all
BGP table version: 4, local router ID is 172.168.201.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, r RIB-failure, S Stale
```



```
*>i0:6:00d0.f822.33df:0:0.0.0.0/128
      2.2.2.2          0      100      0      i
*> 0:6:0011.2233.2016:32:100.1.1.2/128
      0.0.0.0          32768    i
*>i0:6:00d0.f822.33df:32:100.1.1.1/128
      2.2.2.2          0      100      0      i
*> 0:32:1.1.1.1/72  0.0.0.0          32768    i
*>i0:32:2.2.2.2/72  2.2.2.2          0      100      0      i
Total number of prefixes 6
```

The following example displays the routing information of the BGP L2VPN VPLS of the *ve_id:offset*.

```
Ruijie(config)# show bgp l2vpn vpls all 4:0
BGP routing table entry for 100:100:4:0
 77 100
 192.168.250.77 from 192.168.250.77 (0.54.121.150)
   Origin IGP, metric 0, localpref 100, valid, external, best
   Extended Community: RT:1:200 RT:12345:11 SoO:12345:11
SoO:0.0.48.58:11 Unknown:12345:0:11 Layer2:5.0.1500
   ve id: 4 offset: 0 block size: 10 label base: 8196
   Last update: Wed Aug 19 04:06:17 1970
```

The following example displays the neighbor summary information of the BGP L2VPN VPLS peer group.

```
Ruijie(config)# show bgp l2vpn vpls summary
BGP router identifier 192.168.250.8, local AS number 23
BGP table version is 1
2 BGP AS-PATH entries
0 BGP Community entries
0 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor      V  AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down
State/PfxRcd
192.168.250.77 4  77   6         5         1     0   0    00:01:55  11

Total number of neighbors
```

Command	Description
BGP table version	BGP table version.
Local Router ID	Local Router ID. Generally it is a loopback address.
status codes	Status codes:

	s :The route is dampened. d :Shielded route flap. h: Historical routes that no longer available * : Valid routes > : Optimal routes i : IBGP routes r : Fails to install the RIB routing table. S: Old routes.
Origin Codes	Origin Codes: i: IGP. e: EGP. ?: Incomplete.
Network	Routing information in the form aa:bb. The aa here represents site ID and the bb represents label model offset.
Next hop	Next hop IP address.
Metric	Metric value of the represent route (if be displayed.)
LocPrf	Local priority.
Path	AS path that reach the destination network.
Route Distinguisher	RD of VPLS.

Related Commands

Command	Description
N/A	N/A

Platform

Description N/A

5.150 show bgp l2vpn all connections

Use the following command to display connection information of the Kompella VPLS or the VPWS PW.

show bgp l2vpn { vpls | vpws } all connections [vfi vfi_name] [neighbor peer-address [policy [detail]] [site-id id] [detail]

Parameter Description

Parameter	Description
<i>vpls</i>	Displays VPLS information.
<i>vpws</i>	Displays VPWS information.
vfi vfi_name	Displays PW information of the specified VFI instance.
neighbor [peer-address]	Displays information on the Kompella VFI PW connected with neighbor.
neighbor peer-address policy	Displays summarized routing policy information on the BGP neighbor.
neighbor peer-address policy	Displays detailed routing policy information on the BGP

detail	neighbor.
site-id <i>id</i>	Displays all connection information of all VFI instances of the specified site ID.
detail	Displays the detailed L2VPN connection information.

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Use this command to display local configuration and the remote STA information on L2 VFI. If there is no remote STA, only local information is displayed.

Guide

The following example displays the PW connection information of the BGP L2VPN VPLS address family.

```
Ruijie# show bgp l2vpn vpls all connections
vfi: vpls1 (VPLS: vpnid 1)
  Local Site: 1
  Connect-Site  Status  Neighbor  Remote-Label  local-Label
  2              up      2.2.2.2   1024           80000
  3              up      3.3.3.3   1025           9192
  4              up      4.4.4.4   1024           8192
vfi: vpls2 (VPLS: vpnid 2)
  Local Site: 1
  Connect-Site  Status  Neighbor  Remote-Label  local-Label
  2              up      2.2.2.2   1124           80001
  3              up      3.3.3.3   1125           9193
  4              down    4.4.4.4   --             --
Ruijie# show bgp l2vpn vpws all connections
vfi: vpws1 (VPWS: vpnid 3)
  Local Site: 1
  Connect-Site  Status  Neighbor  Remote-Label  Local-Label
  5              up      2.2.2.2   1124           73728
  6              up      3.3.3.3   1125           73729
  7              up      4.4.4.4   1124           73730
```

Configuration Examples

Parameter	Description
vfi	Name of the VFI instance. (n) indicates the VPN ID of the VFI instance.
Local Site	Local site ID.
Connect-Site	Remote site ID.
Status	Whether the PW connection is up or down.
Neighbor	The PW neighbor's IP address.

Remote-Label	The PW remote tag (outbound tag).
Local-Label	The PW local tag (inbound tag).

The following example displays all VFI instance connection information of Site ID 1 of the L2VPN VPWS address family.

```
Ruijie# show bgp l2vpn vpws all connections site 1 detail
```

```
vfi: vpws1 (VPWS:vpnid 1)
```

```
Local site: 1
```

```
Label-base      offset      range
73728           1           10
73738           11          10
```

```
Remote site: 2 (connected)
```

```
Neighbor address: 172.10.10.2
```

```
Label-base      offset      range
9000             1           10
```

```
Incoming label: 73729, Outgoing label: 9000
```

```
Ruijie# show bgp l2vpn vpls all connections site 1 detail
```

```
vfi: vpls1 (VPLS:vpnid 1)
```

```
Local site: 1
```

```
Label-base      offset      range
8192             1           10
8292             11          10
```

```
Remote site: 2 (connected)
```

```
Neighbor address: 172.10.10.2
```

```
Label-base      offset      range
9000             1           10
```

```
Incoming label: 8193, Outgoing label: 9000
```

```
Remote site: 25 (unconnected)
```

```
Neighbor address: 172.10.10.3
```

```
Label-base      offset      range
10000            1           10
```

```
Incoming label: --, Outgoing label: --
```

Parameter	Description
vfi	Name of the VFI instance. (n) indicates the VPN ID of the VFI instance.
Local Site	Local site ID.
Label-base	Label block base.
Offset	Label block offset.
Range	The maximum number of connected sites.
Remote site	Remote site ID. One local site can be connected with multiple remote sites.

	<p>Connected; The remote site is connected with the local site.</p> <p>Unconnected: The remote site is not connected with the local site.</p>
--	---

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.151 show bgp vpnv4 unicast

Use this command to display the VPN or neighbor information of all the VRFs or RDs.

- show bgp vpnv4 unicast all**
- show bgp vpnv4 unicast all *network***
- show bgp vpnv4 unicast all neighbor [*address* [**policy** [**detail**]]]**
- show bgp vpnv4 unicast all summary**
- show bgp vpnv4 unicast all summar**
- show bgp vpnv4 unicast vrf *vrf_name* [*network* | **summary** | **label**]**
- show bgp vpnv4 unicast rd *rd_value* [*network* | **summary**| **label**]**

Parameter Description	Parameter	Description
	<i>network</i>	Network IP address
	neighbor	Displays neighbor information.
	neighbor <i>address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
	neighbor <i>address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
	summary	Displays the route summary information.
	label	Displays the label information of routes.
	<i>vrf_name</i>	VRF name
<i>rd_value</i>	RD value, for example, 100:1 or 202.118.239.165:1	

Defaults N/A

Command Mode Privileged EXEC mode

Usage This command is used to display the VPN information of all VRFs or RDs.

Guide

The following example displays the route information of VPNv4 address family.

```
Ruijie# show bgp vpnv4 unicast all
BGP table version is 0, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Route Distinguisher: 78:90 (Default for VRF this)
  Network   Next Hop   Metric  LocPrf  Path
*> 202.210.10.0 177.36.51.3    0    10  i
*>i208.208.1.0 192.168.195.183  0   100  i
*>i208.208.2.0 192.168.195.183  0   100  i
*> 211.158.0.0 0.0.0.0        0     i
*>i211.158.1.0 192.168.195.183  0   100  i
*> 212.210.0.0 0.0.0.0        0     i
*> 212.210.1.0 0.0.0.0        0     i
Total number of prefixes 7
```

Configuration
Examples

```
Ruijie# show bgp vpnv4 unicast vrf this summary
BGP router identifier 192.168.183.1, local AS number 23
BGP VRF this Route Distinguisher: 78:90
BGP table version is 1
2 BGP AS-PATH entries
1 BGP community entries
Neighbor  V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
177.36.51.2 4 10  0  0  0  0  0 never Active
177.36.51.3 4 10  85  87  1  0  0 01:12:25 5
Total number of neighbors 2
```

Related
Commands

Command	Description
N/A	N/A

Platform
Description

N/A

5.152 show bgp vpnv6 unicast

Use this command to display the VPNv6 or neighbor information of all the VRFs or RDs.

show bgp vpnv6 unicast all

show bgp vpnv6 unicast all *network*

show bgp vpnv6 unicast all neighbor [*address* [**policy** [**detail**]]]

show bgp vpnv6 unicast all summary

show bgp vpnv6 unicast all label

show bgp vpnv6 unicast vrf *vrf_name* [*network* | **summary | **label**]**

show bgp vpnv6 unicast rd *rd_value* [*network* | **summary | **label**]**

Parameter	Description
<i>network</i>	Network IP address
neighbor [<i>address</i>]	Displays the BGP VPNv6 neighbor information. All BGP VPNv6 neighbor information is displayed by default.
neighbor <i>address</i> policy	Displays the summarized BGP neighbor routing policy.
neighbor <i>address</i> policy detail	Displays the detailed BGP neighbor routing policy.
summary	Displays the route summary information.
label	Displays the route label information.
<i>vrf_name</i>	VRF name
<i>rd_value</i>	RD value, for example, 100:1 or 202.118.239.165:1.

**Parameter
Description**

Defaults

N/A

Command

Mode

Privileged EXEC mode

Usage

Use this command to display the VRF that supports IPv6 address family or the VPNv6 routing information of the RD.

Guide

The following example displays all routing information of the VPNv6 address family.

```
Ruijie# show bgp vpnv6 unicast all
BGP table version is 0, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Route Distinguisher: 78:90 (Default for VRF this)
   Network          Next Hop          Metric      LocPrf   Path
*> 10::/64          177.36.51.3        0           10      i
*>i10:1::/64        192.168.195.183    0           100     i
*>i10:2::/64        192.168.195.183    0           100     i
*> 10:3::/64        0.0.0.0            0              i
*>i10:4::/64        192.168.195.183    0           100     i
*> 10:5::/64        0.0.0.0            0              i
*> 10:6::/64        0.0.0.0            0              i
Total number of prefixes 7
```

**Configuration
Examples**

```
Ruijie# show bgp vpnv6 unicast vrf this summary
BGP router identifier 192.168.183.1, local AS number 23
BGP VRF this Route Distinguisher: 78:90
BGP table version is 1
2 BGP AS-PATH entries
1 BGP community entries
Neighbor      V   AS   MsgRcvd  MsgSent  TblVer  InQ   OutQ   Up/Down
State/PfxRcd
20::2         4   10     0        0        0     0     0     never
Active
20::3         4   10    85       87       1     0     0     01:12:25   5
Total number of neighbors 2
```

Parameter	Description
BGP table version	BGP table version.
Local Router ID	Local Router ID. Generally it is an IP address of a loopback interface.
status codes	Status codes: s :The route is dampened. d :Shielded route flap. h: Historical routes that are no long available. * : Valid routes. > : Optimal routes. i : IGBP routes. r : Fails to install the RIB routing table. S: Old routes.
Origin Codes	Origin Codes: i: IGP. e: EGP. ?: Incomplete.
Route Distinguisher	Routing information in the form aa: bb. The aa here represents site ID and the bb represents label model offset.
Network	Next hop IP address.
Next hop	Metric value of the represent route (if be displayed.)
Metric	BGP table version.
LocPrf	Local Router ID, usually it is an IP address of a loopback interface.
Path	The path to the destination AS,

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.153 show ip bgp

Use this command to display the BGP IPv4 unicast address families' route information. The method of use is the same as other BGP show commands.

show ip bgp [*vrf vrf-name*] [*network* [*network-mask* [**longer-prefixes**]] | **cidr-only** | **community** [*community-number* [**exact-match**]] | **filter-list** *path-list-number* | **community-list** *community-name* [**exact-match**] | **regex** *regex* | **quote-regex** *regex* | **extcommunity-list** *extcommunity-name* | **inconsistent-as** | **prefix-list** *ip-prefix-list-name* | **route-map** *map-tag*]

Display route flap's parameters.

show ip bgp [*vrf vrf-name*] **dampening** { **flap-statistics** | **dampened-paths** | **parameters** }

Display neighbors' related information.

show ip bgp [*vrf vrf-name*] **neighbors** [*peer-address* [**received-routes** | **routes** | **advertised-routes** [**policy** [**detail**]]]]

show ip bgp [*vrf vrf-name*] **summary**

Display directory information.

show ip bgp [*vrf vrf-name*] **paths**

Display route scan status.

show ip bgp scan

Display related information under VRF.

show ip bgp vrf *vrf-name*

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name.
<i>network</i>	Displays specific route information in the route table.
<i>network-mask</i>	Displays route information in the specific network.
longer-prefixes	Displays the route map information.
cidr-only	Displays route information without specific category.
community <i>community-number</i>	Displays route information containing specific community value. The <i>community-number</i> is the group number. The format is AA:NN (autonomous system number/2-byte figure), or the following pre-defined value: internet, no-export, local-as or no-advertise.
community-list <i>community-name</i>	Displays the BGP route information of the specified community list. The <i>community-name</i> is the name of the community list.
dampening dampened-paths	Displays dampened route information.
dampening flap-statistics	Displays the route flap statistics.
dampening parameters	Displays believed route flap parameters.
extcommunity-list	Displays route information containing specific extcommunity value.
filter-list <i>path-list-number</i>	Displays the route information that complies with the filter list. The <i>path-list-number</i> is the marking number of the filter list.
inconsistent-as	Displays the route information of inconsistent source AS.
labels	Displays the IPv4 label route information.

neighbors <i>peer-address</i>	Displays the route information of BGP neighbors.
neighbors <i>peer-address</i> received-routes	Displays all routing information received from the specified peer (including accepted and refused routes).
neighbors <i>peer-address</i> routes	Displays all the routing information received from the peer and accepted.
neighbors <i>peer-address</i> advertised-routes	Displays all the routing information sent to the specified peer.
neighbors <i>peer-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
neighbors <i>peer-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
paths	Displays the route information in the route database.
prefix-list	Displays the route information that complies with the prefix list.
quote-regexp <i>regexp</i>	Displays the BGP route information of regular expression in the specified double quotation mark of the AS route attribute.
regexp <i>regexp</i>	Displays the BGP route information of specified regular expression of the AS route attribute.
route-map	Displays the route information that complies with the route map.
scan	Displays the BGP route scanning status.
summary	Displays related information of BGP neighbors.

Defaults -

Command Privileged EXEC mode

Mode

Usage Guide The **show ip bgp** command is the same as **show bgp ipv4 unicast** in terms of the function. All the parameters in **show bgp ipv4 unicast** apply to **show ip bgp**.

Configuration -

Examples

Configuration Examples

Command	Description
show bgp ipv4 unicast	Displays IPv4 unicast route information in BGP route information.

Platform -

Description

5.154 synchronization

Use this command to enable the synchronization mechanism of BGP and IGP routing information. Use the **no** or **default** form of this command to restore the default setting.

synchronization

no synchronization

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

The synchronization between BGP and IGP aims to prevent the possible route black hole. In any of the two cases below, you may cancel the synchronization mechanism to ensure fast convergence of routing information.

Usage Guide

- There is no route information which passes through this AS (In general, this AS is an end AS).
- All devices within this AS operate BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).

Configuration Examples The following example enables the synchronization mechanism of BGP and IGP routing information.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# synchronization
```

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.

Platform Description None

5.155 table-map

Use this command to control the route information distributed to the kernel table. Use the **no** or **default** form of this command to restore the default setting.

table-map *route-map-name*

no table-map

default table-map

Parameter	Parameter	Description
Description	<i>route-map-name</i>	Name of the route-map

Defaults No table-map is configured by default,

Command Mode BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.

Usage Guide BGP uses the table-map to control the information distributed to the kernel routing table. The table-map is used to modify attributes of that route information, and it only takes effect on the IPv4 address-family.

Configuration Examples The following example controls the route information distributed to the kernel table.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# table-map bgp_tm
```

Related Commands	Command	Description
	route-map	Configures the route-map

Platform Description None

5.156 timers bgp

Use this command to adjust the BGP network timer. Use the **no** or **default** form of this command to restore the default value.

timers bgp *keepalive holdtime [minimum-holdtime]*

no timers bgp

default timers bgp

Parameter	Parameter	Description
Parameter Description	<i>keepalive</i>	Time interval to send the keepalive message to the BGP peer Range: 0-65535 seconds.
	<i>holdtime</i>	Time interval to consider the BGP peer alive Range: 0-65535 seconds.
	<i>Minimum-holdtime</i>	Allows a minimum holdtime value of neighbor advertisement. It is unrestricted when the value is 0. The range is 0 to 65535 seconds.

Defaults *keepalive*: 60 seconds

holdtime: 180 seconds
minum-holdtime: 0 seconds

Command

Mode BGP configuration mode / BGP scope global configuration mode

A proper keepalive value must not exceed one-third of the holdtime value.

Usage

If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer.

Guide

If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.

Configuration

The following example adjusts the BGP network timer.

Examples

```
Ruijie(config)# router bgp 65000  
Ruijie(config-router)# timers bgp 80 240
```

Related**Commands**

Command	Description
neighbor timers	Sets the keepalive and holdtime values on the basis of neighbors.

Platform**Description**

None

6 PBR Commands

6.1 clear ip pbr statistics

Use this command to clear the IPv4 PBR forwarded packet count.

clear ip pbr statistics [**interface** *if-name* | **local**]

Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the device clears the IPv4 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv4 PBR forwarded packet count on every interface where IPv4 PBR is enabled.
	local	Clears the IPv4 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to clear the IPv4 PBR forwarded packet count.

Configuration Examples The following example clears the IPv4 PBR forwarded packet count.

```
Ruijie#clear ip pbr statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.2 clear ipv6 pbr statistics

Use this command to clear the IPv6 PBR forwarded packet count.

clear ipv6 pbr statistics [**interface** *if-name* | **local**]

Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the device clears the IPv6 PBR forwarded packet count on that interface.

	Otherwise, the device clears the IPv6 PBR forwarded packet count on every interface where IPv6 PBR is enabled.
local	Clears the IPv6 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to clear the IPv6 PBR forwarded packet count.

Configuration The following example clears the IPv6 PBR forwarded packet count.

Examples

```
Ruijie#clear ipv6 pbr statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.3 ip local policy route-map

Use this command to apply the policy-based routing (PBR) on the packets sent locally. Use the **no** form of this command to restore the default setting.

ip local policy route-map *route-map*

no ip local policy route-map

Parameter Description	Parameter	Description
	<i>route-map</i>	

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

Configuration The following examples send the packets with the source address 192.168.217.10 from the serial 2/0.

Examples The following example defines an ACL that match the IP packet.

```
Ruijie(config)#access-list 1 permit 192.168.217.10
```

The following example defines the route map.

```
Ruijie(config)#route-map lab1 permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set interface serial 2/0
Ruijie(config-route-map)#exit
```

The following example applies PBR on the local interface.

```
Ruijie(config)#ip local policy route-map lab1
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the output port of the policy-based routing.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform N/A

Description

6.4 ip policy

Use this command to set the policy: redundant backup or load balancing used between multiple next hops of the PBR applied for the **set ip [default] nexthop** command in global configuration mode.

Use the **no** form of this command to restore the default setting.


ip policy { load-balance | redundance }
no ip policy

Parameter Description	Parameter	Description
	load-balance redundance	Specifies the policy: load balancing or redundant backup.

Defaults Redundant backup is adopted by default.

Command Mode Global configuration mode

Usage Guide When you configure the **set ip next-hop** command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop of the policy-based routing takes effect. When the load balancing is set, multiple resolved next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops. The resolved next hop refers to the ARP message learned by the next hop and the MAC address corresponding to this ARP exists in the MAC address table.

 NPE80 does not support this command.

Configuration Examples In the example below, there are multiple next hops configured in the route map. After the redundant backup is set in global configuration mode, only the first next hop among the sub-route map of the policy-based routing applied on the interface FastEthernet 0/0 takes effect.

The following example sets the ACL that match the IP packet.

```
Ruijie(config)#access-list 1 permit 10.0.0.1
Ruijie(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
Ruijie(config)#route-map lab1 permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip next-hop 196.168.4.6
Ruijie(config-route-map)#set ip next-hop 196.168.4.7
Ruijie(config-route-map)#set ip next-hop 196.168.4.8
Ruijie(config-route-map)#exit
Ruijie(config)#route-map lab1 permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip next-hop 196.168.5.6
Ruijie(config-route-map)#set ip next-hop 196.168.5.7
Ruijie(config-route-map)#set ip next-hop 196.168.5.8
Ruijie(config-route-map)#exit
```

The following example applies the policy-based routing on the interface.

```
Ruijie(config)#interface FastEthernet 0/0
```



```
Ruijie(config-if)#ip policy route-map lab1
Ruijie(config-if)#exit
Ruijie(config)#ip policy redundance
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

6.5 ip policy route-map

Use this command to apply the policy-based routing on an interface. Use the **no** form of this command to restore the default setting.

ip policy route-map *route-map*

no ip policy route-map


Parameter Description	Parameter	Description
		<i>route-map</i>

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

 Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples In the example below, when the interface FastEthernet0/0 receives a datagram, if the source address of the datagram is 10.0.0.1, it sets the next-hop as 196.168.4.6; if the source address is 20.0.0.1, it sets the next-hop as 196.168.5.6; otherwise, the general forwarding will be performed.

The following example sets the ACL matched with the IP packets.

```
Ruijie(config)#access-list 1 permit 10.0.0.1
Ruijie(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
Ruijie(config)#route-map lab1 permit 10
Ruijie (config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip next-hop 196.168.4.6
Ruijie(config-route-map)#exit
Ruijie(config)#route-map lab1 permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip next-hop 196.168.5.6
Ruijie(config-route-map)#exit
```

The following example applies the route map on the interface.

```
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if)#ip policy route-map lab1
Ruijie(config-if)#exit
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the policy-based routing output port.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform N/A
Description

6.6 ipv6 local policy route-map

Use this command to enable the policy-based routing on the packets sent locally. Use the **no** form of

this command to restore the default setting.

ipv6 local policy route-map *route-map-name*

no ipv6 local policy route-map

**Parameter
Description**

Parameter	Description
<i>route-map-name</i>	Name of the router map applied locally, which is configured by the router-map command.

Defaults

This function is disabled by default.

**Command
Mode**

Global Configuration mode

Usage Guide

- This command is valid only for the IPv6 packets in accordance with the policy (for example, ping packets used for management) sent locally, but not the packets received locally.
- To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

**Configuration
Examples**

The following examples display the PBR application process: The device sends the packets from the source address 2003:1000::10/80 to the 2001:100::/64, the packets will match ACL6 of aaa and be sent to the device 2003:1001::2.

- The following example defines the ACL matched with the IPv6 packet:

```
Ruijie(config)#ipv6 access-list aaa
Ruijie(config)#permit ipv6 2003:1000::10/80 2001:100::/64
```

- The following example defines the router map.

```
Ruijie(config)#route-map pbr-aaa permit 10
Ruijie(config-route-map)#match ipv6 address aaa
Ruijie(config-route-map)#set ipv6 next-hop 2003::1001::2
```

- The following example applies the PBR on the device.

```
Ruijie(config)#ipv6 local policy route-map pbr-aaa
```

**Related
Commands**

Command	Description
match ipv6 address	Sets the ACL6 used to match the IPv6 packets in the IPv6 PBR.
match length	Defines the length of matched packets.
route-map	Defines the route map for PBR.
set default interface	Defines the default next hop output port.
set interface	Defines the next hop output port.

set ipv6 default next-hop	Sets the default next hop of packet forwarding.
set ipv6 next-hop	Sets the next hop of packet forwarding.
set ipv6 precedence	Sets the priority field in the head of IPv6 packets.
show ipv6 policy	Displays the current PBR application.
show route-map	Displays the current router map configuration.

Platform N/A

Description

6.7 ipv6 policy

Use this command to set the policy: redundant backup or load balancing, applied for the **set ip nexthop** command in global configuration mode. Use the **no** form of this command to restore the default setting.

ipv6 policy { load-balance | redundancy }

no ipv6 policy

Parameter Description

Parameter	Description
load-balance	Sets the policy as load balancing.
redundance	Sets the policy as redundant backup.

Defaults Redundant backup is adopted by default.

Command Mode Global configuration mode

Usage Guide This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.


To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

Configuration This function is valid for the multiple next-hops.

Examples When you configure the set ip next-hop command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop takes effect. The second configured next hop will take effect only when the first one fails and the first next hop will take effect again if it recovers.

When the load balancing is set, multiple next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops.

 The resolved next hop refers to the learned MAC address for the next-hop.

The following example sets load-balancing mode for multiple nexthops.

The following example configures an ACL matching with IP packets.

```
Ruijie(config)# ipv6 access-list 1
Ruijie(config-ipv6-acl)# permit ipv6 1000::1 any
Ruijie(config)# ipv6 access-list 2
Ruijie(config-ipv6-acl)# permit ipv6 2000::1 any
```

The following example defines a route map.

```
Ruijie(config)# route-map lab1 permit 10
Ruijie(config-route-map)# match ipv6 address 1
Ruijie(config-route-map)# set ipv6 next-hop 2002::1
Ruijie(config-route-map)# set ipv6 next-hop 2002::2
Ruijie(config-route-map)# set ipv6 next-hop 2002::3
Ruijie(config-route-map)# exit
Ruijie(config)# route-map lab1 permit 20
Ruijie(config-route-map)# match ipv6 address 2
Ruijie(config-route-map)# set ipv6 next-hop 2002::5
Ruijie(config-route-map)# set ipv6 next-hop 2002::6
Ruijie(config-route-map)# set ipv6 next-hop 2002::7
Ruijie(config-route-map)# exit
```

The following example applies policy-based routing on the interface.

```
Ruijie(config)# interface FastEthernet 0/0
Ruijie(config-if)# ipv6 policy route-map lab1
Ruijie(config-if)# exit
Ruijie(config)# ipv6 policy load-balance
```

Related Commands

Command	Description
set ipv6 default next-hop	Defines the default next hop for forwarding the packets.
set ipv6 next-hop	Defines the next hop for forwarding the packets.
show ipv6 policy	Displays the current policy-based routing application.

Platform N/A

Description

6.8 ipv6 policy route-map

Use this command to apply the policy-based routing on an interface in interface configuration mode.

Use the **no** form of this command to restore the default setting.

ipv6 policy route-map *route-map-name*

no ip policy route-map

**Parameter
Description**

Parameter	Description
<i>route-map-name</i>	Name of the PBR router map applied locally, which is configured by the router-map command.

Defaults

This function is disabled by default..

Command


Interface configuration mode

Mode

Usage Guide

The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

 Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration

An IPv6 packet is received on the fastEthernet 0/0. If the packet is sent from 10::/64 network

Examples

segment, it is forwarded to the next hop of 2000:1; if the packet is sent from 20::/64 network segment, it is forwarded to the next hop of 2000:2 or forwarded as usual.:

The following example configures an ACL matched with the IP packet.

```
Ruijie(config)# ipv6 access-list acl_for_pbr1
Ruijie (config-ipv6-acl)# permit ipv6 10::/64 any
Ruijie(config)# ipv6 access-list acl_for_pbr2
Ruijie (config-ipv6-acl)# permit ipv6 20::/64 any
```

The following example defines a route map.

```
Ruijie(config)# route-map rm_pbr permit 10
Ruijie (config-route-map)# match ipv6 address acl_for_pbr1
Ruijie(config-route-map)# set ipv6 next-hop 2000::1
Ruijie(config-route-map)# exit
Ruijie(config)# route-map rm_pbr permit 20
Ruijie(config-route-map)# match ipv6 address acl_for_pbr2
Ruijie(config-route-map)# set ipv6 next-hop 2000::2
Ruijie(config-route-map)# exit
```

The following example applies the route map to the interface.

```
Ruijie(config)# interface FastEthernet 0/0
```

```
Ruijie(config-if)# no switchport
Ruijie(config-if)# ipv6 policy route-map rm_pbr
Ruijie(config-if)# exit
```

**Related
Commands**

Command	Description
route-map	Defines the route map.
match ipv6 address	Sets the IPv6 ACL used to match the IPv6 packets in the IPv6 PBR.
set ipv6 default next-hop	Defines the default next hop of the packet forwarding.
set ipv6 next-hop	Defines the next hop of the packet forwarding.
show ipv6 policy	Displays the current policy-based routing application.
show route-map	Displays the current route map configurations.

Platform N/A

Description

6.9 show ip pbr bfd

Use this command to display the correlation between the IPv4 policy router and BFD.

show ip pbr bfd

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the correlation between the IPv4 policy router and BFD.

Examples

```
Ruijie# show ip pbr bfd
VRF ID  Ifindex  Host                State  Refcnt
   0      13  192.168.8.100      Up      2
```

Field Description

Field	Description
VRF ID	VRF of BFD neighbors correlated with the policy router

Ifindex	The interface index of BFD neighbors correlated with the policy router
Host	The peer IPv4 address
State	Up/Down status of BFD neighbors correlated with the policy router
Refcnt	Calculation referred by BFD neighbors

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

6.10 show ip pbr route

Use this command to display the IPv4 PBR information on the interface.

show ip pbr route [**interface** *if-name* | **local**]

**Parameter
Description**

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv4 BPR information of this interface is displayed. Otherwise, the IPv4 BPR information of all interfaces where the IPv4 PBR is enabled is displayed.
local	Displays the IPv4 PBR information on the local interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IPv4 PBR information.

Configuration The following example displays the IPv4 PBR information on the interfaces.

Examples

```
Ruijie#show ip pbr route
PBR IPv4 Route Summay : 1
Interface      : GigabitEthernet 0/1
  Sequence    : 10
  ACL[0]      : 2900
ACL_CLS[0]    : 0
  Min Length  : None
  Max Length  : None
```



```

VRF ID      : 0
Route Flags :
Route Type  : PBR
Direct      : Permit
Priority     : High
Tos_Dscp    : None
Precedence  : None
Tos_Dscp    : 0
Precedence  : 0
Mode        : redundance
Nexthop Count : 1
Nexthop[0]  : 192.168.8.100
Weight[0]   : 1
Ifindex[0]  : 2

```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
Min Length	The minimum match length.
Max Length	The maximum match length.
VRF ID	Port-correlated VRF ID.
Route Flags	<p>PBR flag bit:</p> <p>Route Type: "PBR" indicates PBR routes. "Normal" indicates common routes.</p> <p>Direct: PBR matching action, permit or deny</p> <p>Priority: PBR priority, High or Low</p> <p>Tos_Dscp: Displays whether the tos rule or the dscp rule is configured.</p> <p>Precedence: Displays whether the set ip precedence rule is configured.</p>
Mode	Specifies the redundancy mode or the next hop load balancing mode.
Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
Nexthop	Specifies the next hop IP address.
Weight	Specifies the next hop weight.
Ifindex	Specifies the outbound interface index corresponding to the next hop.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

6.11 show ip pbr route-map

Use this command to display the IPv4 PBR route-map information.

show ip pbr route-map *route-map-name*

Parameter Description	Parameter	Description
		<i>route-map-name</i>

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the IPv4 PBR route-map information.

Examples

```
Ruijie#show ip pbr route-map rm
Pbr VRF: GLOBAL, ID: 0
  Forward Mode: redundance
  Forwarding: On

route-map rm
  route-map index: sequence 10, permit
  Match rule:
    ACL ID :      0, ACL CLS: 0, Name: acl1
  Set rule:
    IPv4 Nexthop: 192.168.8.100, (VRF Name: , ID: 0), Weight: 0, Flags: 0
    PBR state info ifx: GigabitEthernet 0/1, Connected: true, Track State:
valid, Flags: 0
```

Field	Description
Pbr VRF	VRF name and VRF ID.
Forward Mode	Sets the load balance mode or the redundancy mode for the next hop.
Forwarding	Displays whether the IP route forwarding is enabled.

Route-map index	The serial number and the type of the sub-map.
Match rule	Match rule.
Set rule	Set rule.
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

6.12 show ip pbr statistics

Use this command to display the IPv4 PBR forwarded packet count.

show ip pbr statistics [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv4 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv4 PBR forwarded packet count of all interfaces where the IPv4 PBR is enabled is displayed.
local	Displays the IPv4 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the IPv4 PBR forwarded packet count.

Examples

```
Ruijie#show ip pbr statistics
IPv4 Policy-based route statistic
gigabitEthernet 0/1
statistics : 10
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

6.13 show ip policy

Use this command to display the interface configured with the policy-based routing and the name of route map applied on the interface.

show ip policy [*route-map-name*]

Parameter Description	Parameter	Description
	<i>route-map-name</i>	Indicates the name of a route map.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to verify the current PBR configured in the system.

Configuration The following example displays the current PBR configured in the system.

Examples

```
Ruijie#show ip policy
Banlance Mode: redundance
Interface      Route map
local         test
FastEthernet 0/0  test
```

Related Commands	Command	Description
	ip policy route-map	Applies the policy-based routing on the interface.
	ip local policy route-map	Applies the policy-based routing on the local interface.

Platform N/A

Description

6.14 show ipv6 pbr bfd

Use this command to display the correlation between the IPv6 policy router and BFD.

show ipv6 pbr bfd

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the correlation between the IPv6 policy router and BFD.

Examples

```
Ruijie# show ipv6 pbr bfd
```

```
VRF ID Ifindex Host State Refcnt
0 13 2000::2 Up 1
```

Field Description

Field	Description
VRF ID	VRF of BFD neighbors correlated with the policy router
Ifindex	The interface index of BFD neighbors correlated with the policy router
Host	The peer IPv6 address
State	Up/Down status of BFD neighbors correlated with the policy router
Refcnt	Calculation referred by BFD neighbors

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.15 show ipv6 pbr route

Use this command to display the IPv6 PBR information on the interface.

show ipv6 pbr route [**interface** *if-name* | **local**]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv6 BPR information of this interface is displayed. Otherwise, the IPv6 BPR information of all interfaces where the IPv6 PBR is enabled

	is displayed.
local	Displays the IPv6 PBR information on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the IPv6 PBR information on the interfaces.

Examples

```
Ruijie#show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface      : GigabitEthernet 0/2
  Sequence     : 10
  ACL[0]       : 2901
ACL_CLS[0]    : 0
  Min Length   : None
  Max Length   : None
  VRF ID       : 0
Route Flags   :
  Route Type   : PBR
  Direct       : Permit
  Priority      : High
  Tos_Dscp     : None
  Precedence   : None
Tos_Dscp      : 0
Precedence    : 0
Mode          : redundance
Nexthop Count : 1
  Nexthop[0]   : 10::1
  Weight[0]    : 1
  Ifindex[0]   : 3
```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
Min Length	The minimum match length.
Max Length	The maximum match length.
VRF ID	Port associated VRF ID.

Route Flags	<p>PBR flag bit:</p> <p>Route Type: "PBR" indicates PBR routes. "Normal" indicates common routes.</p> <p>Direct: PBR matching action, permit or deny</p> <p>Priority: PBR priority, High or Low</p> <p>Tos_Dscp: Displays whether the tos rule or the dscp rule is configured.</p> <p>Precedence: Displays whether the set ip precedence rule is configured.</p>
Mode	Specifies the redundancy mode or the load balance mode for the next hop.
Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
Nexthop	Specifies the next hop IP address.
Weight	Specifies the next hop weight.
Ifindex	Specifies the outbound interface index corresponding to the next hop

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

6.16 show ipv6 pbr route-map

Use this command to display the IPv6 PBR route-map information.

show ipv6 pbr route-map *route-map-name*

**Parameter
Description**

Parameter	Description
<i>route-map-name</i>	The route-map name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the IPv6 PBR route-map information.

Examples

```
Ruijie#show ipv6 pbr route-map rm6
Pbr VRF: GLOBAL, ID: 0
  Forward Mode: redundance
  Forwarding: On

route-map rm6
  route-map index: sequence 10, permit
Match rule:
  ACL ID :      0, ACL CLS: 0, Name: acl6
  Set rule:
    IPv6 Nexthop: 10::1, (VRF Name: , ID: 0), Weight: 0, Flags: 0
    PBR state info ifx: GigabitEthernet 0/0, Connected: true, Track State:
valid, Flags: 0
```

Field	Description
Pbr VRF	VRF name and VRF ID.
Forward Mode	Sets the load balancing mode or to the redundancy mode for the next hop.
Forwarding	Displays whether the IP route forwarding is enabled.
Route-map index	The serial number and the type of the sub-map.
Match rule	Match rule
Set rule	Set rule.
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

6.17 show ipv6 pbr statistics

Use this command to display the IPv6 PBR forwarded packet count.

show ip pbr statistics [interface *if-name* | local]

Parameter Description

Parameter	Description
interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv6 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv6 PBR forwarded packet count of all interfaces

	where the IPv6 PBR is enabled is displayed.
local	Displays the IPv6 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the IPv6 PBR forwarded packet count.

Examples

```
Ruijie#show ipv6 pbr statistics
IPv6 Policy-based route statistic
gigabitEthernet 0/1
  statistics : 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.18 show ipv6 policy

Use this command to display which interfaces are configured with IPv6 PBR.

show ipv6 policy [*route-map-name*]

Parameter Description

Parameter	Description
<i>route-map-name</i>	Name of the PBR router map.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the current PBR applied in the system.

Examples

```
Ruijie#show ipv6 policy
Banlance Mode: redundance
Interface          Route map
VLAN 1             RM_for_Vlan_1
VLAN 2             RM_for_Vlan_2
```

Field	Description
Balance Mode	The current PBR running mode.
Interface	The name of interface with PBR applied.
Route map	The name of route map applied on the interface.

**Related
Commands**

Command	Description
show route-map	Displays the current configured route map.

Platform

N/A

Description

7 VRF Commands

7.1 address-family

Use this command to configure an IPv4 address family or IPv6 address family for a multiprotocol VRF.

address-family { *ipv4* | *ipv6* }

Parameter Description	Parameter	Description
	ipv4	Enters IPv4 address family.
	ipv6	Enters IPv6 address family.

Defaults No IPv4 address family or IPv6 address family is configured for a multiprotocol VRF.

Command mode VRF configuration mode

Usage Guide This command is applicable only to the multiprotocol VRF.

Configuration Examples The following example defines a multiprotocol VRF vrf1 and configures an IPv4 address family.

```
Ruijie(config)#vrf definition vrf1
Ruijie(config-vrf)#address-family ipv4
Ruijie(config-vrf-af)#
```

Related Commands	Command	Description
	exit-address-family	Exits the VRF address family configuration mode.
	vrf definition	Defines a multiprotocol VRF.

Platform Description N/A

7.2 description

Use this command to configure the VRF description.

description *string*

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>string</i>	VRF description character string. The maximum length is 244 characters.
---------------	---

Defaults No VRF description is configured by default .

Command mode VRF configuration mode

Usage Guide N/A

Configuration Examples The following example defines a single-protocol IPv4 VRF vrf1 and configure the description to vpn-a.

```
Ruijie(config)#ip vrf definition vrf1
Ruijie(config-vrf)#description vpn-a
```

The following example defines a multiprotocol VRF vrf2 and configure the description to vpn-b.

```
Ruijie(config)#vrf definition vrf1
Ruijie(config-vrf)#description vpn-b
```

Related Commands

Command	Description
ip vrf	Defines a single-protocol IPv4 VRF.
vrf definition	Defines a multiprotocol VRF.

Platform Description N/A

7.3 exit-address-family

Use this command to exit VRF address family configuration mode.

exit-address-family

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode VRF address family configuration mode

Usage Guide N/A

Configuration Examples The following example defines a multiprotocol VRF vrf1 and configures an IPv4 address family.

```
Ruijie(config)#vrf definition vrf1
```

```
Ruijie(config-vrf)#address-family ipv4
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config-vrf)#
```

**Related
Commands**

Command	Description
address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol VRF.
vrf definition	Defines a multiprotocol VRF.

Platform N/A
Description

7.4 ip vrf

Use this command to create a VRF. Use the **no** form of this command to delete a VRF.

ip vrf *vrf-name*
no ip vrf *vrf-name*

**Parameter
Description**

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults No VRF is configured by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example creates a VRF.

```
Ruijie(config)# ip vrf redvrf
Ruijie(config-vrf)#
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

7.5 ip vrf forwarding

Use this command to add an interface or sub-interface to a VRF. Use the **no** form of this command to quit the VRF.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Parameter Description	Parameter	Description
	<i>vrf-name</i>	Name of the VRF that the interface or sub-interface joins

Defaults By default, the interface does not belong to any VRF.

Command mode Interface configuration mode

Usage Guide You can bind the interface to the uni-protocol IPv4 VRF without the IPv6 enabled on the interface. On the device supporting the VRF, if the interface is bound to the uni-protocol IPv4 VRF with the IPv6 protocol enabled, the device cannot forward the IPv6 packets received on this interface.

Configuration The following example adds an interface or sub-interface to a VRF.

Examples Ruijie (config-if-GigabitEthernet 0/0) # ip vrf forwarding redvrf

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

7.6 ip vrf receive

Use this command to import the host and direct-connected route of one interface into the specified VRF routing table. Use the **no** form of this command to remove the imported host and direct-connected route from the VRF.

ip vrf receive *vrf-name*

no ip vrf receive *vrf-name*

Parameter Description	Parameter	Description
	<i>vrf-name</i>	Name of the VRF that the host and direct-connected route imported to.

Defaults By default, the host and direct-connected route of the interface are not imported to other VRFs

Command mode Interface configuration mode

Usage Guide Currently, the **ip vrf receive** command supports the VRF routing based on the PBR. This command is used to import the host with the main and slave addresses and direct-connected route of this interface into the specified VRF routing table. You need to execute this command multiple times to import this host and direct-connected route to multiple VRF routing tables. Unlike the **ip vrf forwarding** command, which does not bind the interface to the VRF and this interface still belongs to the global VRF. Configuring both **ip vrf forwarding** and **ip vrf receive** on an interface is not allowed. If one has been configured, configuring the other one will prompt an error message.

If **ip vrf forwarding** has been configured, configuring **ip vrf receive** will prompt:

```
% Cannot configure 'ip vrf receive' if interface is under a VRF
```

If **ip vrf receive** has been configured, configuring **ip vrf forwarding** will prompt:

```
% Cannot bind interface to a VRF if it has configed 'ip vrf receive'
```

Configuration Examples The following example imports the host and direct-connected route of one interface into the specified VRF routing table.

```
Ruijie(config)# interface FastEthernet0/1
Ruijie(config-if)# ip address 192.168.1.2 255.255.255.0
Ruijie(config-if)# ip policy route-map PBR-VRF-SELECTION
Ruijie(config-if)# ip vrf receive VRF_1
Ruijie(config-if)# ip vrf receive VRF_2
Ruijie(config-if)# end
```

Related Commands

Command	Description
ip vrf forwarding	Adds the interface to a VRF.
ip vrf	Creates a VRF.
set vrf	Sets the VRF in the routing map configuration mode.

Platform N/A

Description

7.7 maximum routes

Use this command to set the maximum routes limit within the VRF. Use the **no** form of this command to remove the setting.

maximum routes *limit* { *warn-threshold* | **warning-only** }

no maximum routes

Parameter

Parameter	Description
-----------	-------------

Description	
<i>limit</i>	The maximum number of routes, in the range from 1 to 4,294,967,295. The routes which exceed the limits will not be added to the core routing table.
<i>warn-threshold</i>	The warning will be printed when the threshold is reached. The threshold value is in the range from 1 to 100.
warning-only	After the number of routes reaches <i>limit</i> , the warning will be printed but the routes will be added to the core routing table.

Defaults N/A

Command Mode Single-protocol VRF is configured in VRF configuration mode; multiple-protocol VRF is configured in address family mode.

Usage Guide This command is used to set the maximum number of routes for the VRF.

Configuration Examples The following example sets the maximum number of routes for vrf1 to 1,000, and enables the device to only print the warning.

```
Ruijie(config)# ip vrf vrf1
Ruijie(config-vrf)# maximum routes 1000 warning-only
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.8 show ip vrf

Use this command to display the VRF information.

show ip vrf [brief | detail | interfaces] [vrf-name]

Parameter Description	Parameter	Description
	brief	(Optional) Displays the VRF information in brief.
detail	(Optional) Displays the VRF information in detail.	
interfaces	(Optional) Displays the VRF's interface information in detail.	
<i>vrf-name</i>	(Optional) Name of the VRF	

Defaults All VRF information is displayed without parameter specified.

Command Privileged EXEC mode

mode

Usage Guide Use this command to display the VRF information, which can be divided into two levels:
 Use the keyword **brief** to display the information in brief.
 Use the keyword **detail** to display the information in detail.
 Use the keyword **interfaces** to display the VRF's interface information.

Configuration The following example displays the VRF information.

Examples

```
Ruijie#show ip vrf
Name                               Interfaces
aaa                                 GigabitEthernet 0/0
                                   GigabitEthernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

7.9 show vrf

Use this command to display the VRF configuration (including the single-protocol VRF and the multiple-protocol VRF).

show vrf [**ipv4** | **ipv6** | **brief** | **count** | **detail**] [*vrf-name*]

Parameter Description

Parameter	Description
ipv4	Displays the brief VRF (the single-protocol VRF) information of the IPv4 address family.
ipv6	Displays the VRF brief information of the IPv6 address family.
brief	Displays the brief VRF (including the single-protocol VRF and the multiple-protocol) information.
count	Displays the capacity of VRF and its current value.
detail	Displays the detailed VRF (including the single-protocol VRF and the multiple-protocol) information.
<i>vrf-name</i>	VRF name.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays brief information about all VRF.

Examples

```
Ruijie#show vrf
```

```

Name          Default RD      Protocols  Interfaces
aaa           <not set>      ipv4
aab           <not set>
bbb           <not set>      ipv6
ccc           <not set>      ipv4,ipv6  V11

```

:

Field	Description
Name	VRF name.
Default RD	Default RD of the VRF.
Protocol	The address family of the VRF. IPv4 indicates the VRF is enabled in the IPv4 address family mode; ipv6 indicates the VRF is enabled in the IPv6 address family mode.
Interfaces	The interface list of the VRF. The interface where the [ip] vrf forwarding command has been configured will be displayed on that list.

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

7.10 vrf definition

Use this command to create the multiprotocol VRF.

vrf definition *vrf-name*

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name, no more than 31 characters.

Defaults

N/A

Command mode

Global configuration mode

Usage Guide The single-protocol VRF configuration command **ip vrf** cannot be used to edit a multiprotocol VRF; the multiprotocol VRF configuration command **vrf definition** cannot be used to edit a single-protocol IPv4 VRF.

Configuration The following example s creates a multiprotocol VRF *vrf1*.

```
Examples Ruijie(config)#vrf definition vrf1
Ruijie(config-vrf)#
```

**Related
Commands**

Command	Description
description	Configures the description.
address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol VRF.
exit-address-family	Exits the VRF address family configuration mode.
vrf forwarding	Binds a network interface to a multiprotocol VRF.

Platform N/A

Description

7.11 vrf forwarding

Use this command to bind a network interface to a multiprotocol VRF.

vrf forwarding *vrf-name*

**Parameter
Description**

Parameter	Description
<i>vrf-name</i>	VRF name, which shall be a multiprotocol VRF instead of a single-protocol VRF that supports IPv4 only.

Defaults The network interface is not bound to any VRF.

Command mode Interface configuration mode

Usage Guide The configuration command **ip vrf forwarding** cannot be used to bind a network interface to a multiprotocol VRF; the configuration command **vrf forwarding** cannot be used to bind a network interface to a single-protocol IPv4 VRF.

An interface cannot be bound to a multiprotocol VRF that is not configured with any address family. To bind a network interface to a multiprotocol VRF, you should delete the existing IPv4 addresses, VRRP IPv4 addresses, IPv6 addresses and VRRP IPv6 addresses, and disable IPv6 on the interface. When a network interface is bound to a multiprotocol VRF, no IPv4 address or VRRP IPv4 address should be configured for the interface if no IPv4 address family is configured for the VRF. You should

configure an IPv4 address family for the VRF before configuring an IPv4 address and VRRP IPv4 address for the interface.

When a network interface is bound to a multiprotocol VRF, no IPv6 address or VRRP IPv6 address should be configured for the interface if no IPv6 address family is configured for the VRF. You should configure an IPv6 address family for the VRF before configuring an IPv6 address and VRRP IPv6 address for the interface.

If you delete a multiprotocol VRF's IPv4 address family, you should delete the IPv4 addresses and VRRP IPv4 addresses of all network interfaces bound to the VRF, and delete the IPv4 static routes whose routing VRF or next-hop VRF is that VRF. Likewise, if you delete a multiprotocol VRF's IPv6 address family, you should delete the IPv4 addresses and VRRP IPv6 addresses of all network interfaces bound to the VRF, disable IPv6 on the interfaces, and delete the IPv6 static routes whose routing VRF or next-hop VRF is that VRF.

Configuration The following example binds the interface VLAN 1 to a multiprotocol VRF vrf1.

Examples

```
Ruijie(config)#vrf definition vrf1
Ruijie(config-vrf)#address-family ipv4
Ruijie(config-vrf-af)#exit-address-family
Ruijie(config-vrf)#address-family ipv6
Ruijie(config-vrf-af)#exit-address-family

Ruijie(config-vrf)#interface vlan 1
Ruijie(config-if)#vrf forwarding vrf1
Ruijie(config-if)#ip address 1.1.1.1 255.255.255.0
Ruijie(config-if)#ipv6 address 1000::1/64
```

**Related
Commands**

Command	Description
vrf definition	Defines a multiprotocol VRF.

Platform N/A

Description

7.12 vrf receive

Use this command to add the local host's route and direct route with the interface's IPv4/v6 address to the routing table of the specified VRF.

vrf receive *vrf-name*

**Parameter
Description**

Parameter	Description
<i>vrf-name</i>	VRF name, which should be a multiprotocol VRF instead of a single-protocol IPv4 VRF.

Defaults N/A

Command mode Interface configuration mode

Usage Guide This command is not used to bind an interface to a VRF, and the interface is still a global interface. If the administrator needs to use PBR to choose VRF, the **vrf receive** command should be configured on the interfaces where PBR is applied for each selected VRF. When an IPv4 address family is configured for a multiprotocol VRF, the local host's route and direct route with the interface's IPv4 address is added to the IPv4 routing table of the specified VRF, and the local host's route with the IPv4 address of the master VRRP group on the interface is added to the IPv4 routing table of the specified VRF. When an IPv6 address family is configured for a multiprotocol VRF, the local host's route and direct route with the interface's IPv6 address is added to the IPv6 routing table of the specified VRF, and the local host's route with the IPv6 address of the master VRRP group on the interface is added to the IPv6 routing table of the specified VRF. The **ip vrf forwarding** and **vrf receive** commands are mutually exclusive on an interface, and so are the **vrf forwarding** and **vrf receive** commands. If both commands are configured on an interface, an error message will be shown.

If the **ip vrf forwarding** or **vrf forwarding** command is configured first, and then the **vrf receive** command is configured, the following message will be displayed:

```
% Cannot configure 'vrf receive' if interface is under a VRF
```

If the **vrf receive** command is configured first, and then the **ip vrf forwarding** or **vrf forwarding** command is configured, the following message will be displayed:

```
% Cannot configure 'vrf forwarding vrf2' on this interface, please delete 'ip vrf receive' and 'vrf receive' first.
```

Configuration Examples The following example selects a VRF using IPv6 PBR on VLAN 1.

```
Ruijie(config)#vrf definition vrf1
Ruijie(config-vrf)#address-family ipv6
Ruijie(config-vrf-af)#exit-address-family

Ruijie(config-vrf)#vrf definition vrf2
Ruijie(config-vrf)#address-family ipv6
Ruijie(config-vrf-af)#exit-address-family

Ruijie(config-vrf)#route-map pbr-vrf-selection permit 10
Ruijie(config-route-map)#match ipv6 address acl1
Ruijie(config-route-map)#set vrf vrf1
Ruijie(config-route-map)#route-map pbr-vrf-selection permit 20
Ruijie(config-route-map)#set vrf vrf2

Ruijie(config-route-map)#interface vlan 1
Ruijie(config-if)#ipv6 policy route-map pbr-vrf-selection
Ruijie(config-if)#ipv6 address 1000::1/64
Ruijie(config-if)#vrf receive vrf1
```

```
Ruijie(config-if)#vrf receive vrf2
```

**Related
Commands**

Command	Description
vrf definition	Defines a multiprotocol VRF.
address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol VRF.
set vrf	Configures a VRF in the route map configuration mode.

**Platform
Description**

N/A

8 RIPng Commands

8.1 clear ipv6 rip

Use this command to clear the RIPng routes.

clear ipv6 rip

Parameter Description	Parameter	Description
	N/A	N/A

Defaults None

Command mode Privileged EXEC mode

Usage Guide Running this command removes all RIPng routes and this operation may have great impact on the RIPng protocol. This command should be used with caution.

Configuration The following example clears the RIPng routes:

Examples

```
Ruijie# clear ipv6 rip
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.2 default-metric

Use this command to configure the default metric for RIPng. Use the **no** form of this command to restore the default value.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
<i>metric</i>	Sets the default metric value. The valid range is from 1 to 16. The route is unreachable if the metric value is larger than or equal to 16.

Defaults

The default value is 1.

Command mode

Routing process configuration mode.

Usage Guide

This command shall be used with the **redistribute** command. When redistributing the route from one route process to RIPng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPng metric value shall be defined when translating the metric values. If there is no defined metric value, use the **default-metric** command to define one; and the defined metric value will overwrite the value of the **default-metric** command. By default, the **default-metric** value is 1.

Configuration Examples

The following example shows how to set the RIPng metric value as 3 when redistributing OSPF process 100:

```
Ruijie(config-router)# default-metric 3
Ruijie(config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the route from one route domain to another route domain.

Platform N/A
Description

8.3 distance

Use this command to set the administrative distance of RIPng. Use the **no** form of this command to restore the default value.

distance *distance*

no distance

Parameter Description	Parameter	Description
		<i>distance</i>

Defaults The default distance is 120

Command mode Routing process configuration mode.

Usage Guide N/A

Configuration The following example shows how to set the RIPng administrative distance as 160:

Examples

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distance 160
```

Related Commands	Command	Description
		N/A

Platform N/A

Description

8.4 distribute-list

Use this command to filter the in/out route in the prefix list. Use the **no** form of this command to remove route filtering.

distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

no distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

Parameter Description

Parameter	Description
prefix-list <i>prefix-list-name</i>	Name of the prefix list which is used to filter the route.
in out	Filters the in or out route in the distribute list.
<i>interface-type</i> <i>interface-name</i>	(Optional) Applies the distribute list to the specified interface.

Defaults By default, no distribute list is defined.

Command mode Routing process configuration mode.

Usage Guide This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.

Configuration Examples The following example shows how to filter the received update route on the interface eth0 (only those update routes within the **prefix-list allowpre** prefix list range can be received)

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distribute-list prefix-list allowpre in eth0
```

Related Commands

Command	Description
---------	-------------

redistribute	Sets route redistribution.
---------------------	----------------------------

Platform N/A

Description

8.5 graceful-restart

Use this command to configure the graceful restart (GR) function for the RIPng process.

graceful-restart [**grace-period** *grace-period*]

Use the **no** form of this command restore the default configurations.

no graceful-restart [**grace-period**]

Parameter Description	Parameter	Description
	graceful-restart	Enables the GR function.
	grace-period	Displays the configured grace period.
	<i>grace-period</i>	Indicates the configured GR period, ranging from 1 to 1800 seconds. The default value is the smaller between twice of the update time and 60s.

Defaults The GR function is enabled by default.

Command Mode Routing process configuration mode

Default Level 14

Usage Guide The GR function is configured based on RIPng instances. Different parameters can be configured for different RIPng instances as required.

The GR period indicates the maximum duration from RIPng restart to RIPng GR completion. In this time period, the forwarding table before restart is used and the RIPng route is restored to the status before

restart. After the GR period expires, the RIPng process exits the GR status and the common RIPng operation is performed.

The **graceful-restart grace-period** command allows a user to modify the GR period in explicit mode. Note that GR is completed and the RIPng route is updated once before the RIPng route becomes invalid. If the GR period is improperly set, continuous data forwarding in the GR process cannot be ensured. A typical case is as follows:

If the GR period is greater than the invalid time of the neighbor route, GR is not completed before the route becomes invalid and the route is not advertised to the neighbor again. The neighbor route stops forwarding data after the route becomes invalid, resulting in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the GR period needs to be configured, check configuration of the **timers** command to ensure that the GR period value is greater than the route update time and smaller than the route invalid time.

When GR is performed for the RIPng process, ensure that the network environment is stable.

Configuration The following example enables the GR function for the RIPng process and configures the GR period.

Examples

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

Verification Run the **show ipv6 rip** command to check whether the GR function is configured and query the configured grace period.

Prompts N/A

Common Errors N/A

Platform Description N/A

8.6 ipv6 rip default-information

Use this command to generate a default IPv6 route to the RIPng. Use the **no** form of this command to remove the default route.

```
ipv6 rip default-information { only | originate } [ metric metric-value ]
```

```
no ipv6 rip default-information
```

Parameter Description	Parameter	Description
	only	Advertises the IPv6 default route only.
	originate	Advertises both of the IPv6 default route and other routes.
	metric <i>metric-value</i>	Sets the metric value for the default route. The valid range is from 1 to 15. The default metric is 1.

Defaults By default, no default route is configured.

Command mode Interface configuration mode

Usage Guide With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPng route database.

To avoid the route loop, once this command has been configured on the interface, RIPng refuses to receive the default route update message advertised from the neighbor.

Configuration Examples The following example shows how to create a default route to the RIPng routing process on the interface ethernet0/0 and enable this interface to advertise the default route only:

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 rip default-information only
```

Related Commands	Command	Description
	show ipv6 rip	Displays the RIPng process and statistics.
	show ipv6 rip database	Displays the RIPng route.

Platform Description N/A

8.7 ipv6 rip enable

Use this command to enable the RIPng on the interface. Use the **no** form of this command to disable RIPng on the interface.

ipv6 rip enable

no ipv6 rip enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults It is disabled by default.

Command mode Interface configuration mode.

Usage Guide This command is used to add the RIPng interface. Before this command is configured, if the RIPng is not enabled, use this command to enable the RIPng automatically.

Configuration Examples The following example shows how to enable the RIPng on the interface 0/0:

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 rip enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.8 ipv6 rip metric-offset

Use this command to set the interface metric value. Use the **no** form of this command to remove the metric configurations.

ipv6 rip metric-offset *value*

no ipv6 rip metric-offset

Parameter Description	Parameter	Description
	<i>value</i>	Sets the interface metric value on the interface. The valid range is from 1 to 16.

Defaults The default value is 1.

Command mode Interface configuration mode.

Usage Guide Before the route is added to the routing list, the interface metric value shall be upon the route metric. To this end, the interface metric value influences the route usage.

Configuration Examples The following example shows how to set the metric value of the interface Ethernet 0/1 as 5:

```
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ipv6 rip metric-offset 5
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.9 ipv6 rip subvlan

Use this command to enable RIPng on super VLANs. Use the **no** form of this command to restore the default setting.

ipv6 rip subvlan [*all* | *vid*]

no ipv6 rip subvlan

Parameter Description

Parameter	Description
<i>all</i>	Indicates that packets are allowed to be sent to all sub VLANs.
<i>vid</i>	Specifies the sub VLAN ID. The value ranges from 1 to 4094.

Defaults

The default setting takes effect only on super VLANs with RIPng disabled.

Command Mode

Interface configuration mode.

Usage Guide

In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIPng multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIPng multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the RIPng function does not need to be enabled on a super VLAN. Therefore, the RIPng function is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration Examples

The following example sends the RIPng multicast packets to sub VLAN 1024 of super VLAN 300.

Examples

```
Ruijie(config)# interface vlan 300
Ruijie(config-if-VLAN 300)# ipv6 rip subvlan 1024
```

8.10 ipv6 router rip

Use this command to create the RIPng process and enter routing process configuration mode. Use

the **no** form of this command to remove the RIPng process.

ipv6 router rip

no ipv6 router rip

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults No RIPng process is configured by default.

Command mode Global configuration mode.

Usage Guide N/A.

Configuration Examples The following example shows how to create the RIPng process and enter routing process configuration mode:

```
Ruijie(config)# ipv6 router rip
```

**Related
Commands**

Command	Description
ipv6 rip enable	Enables the RIPng on the specified interface.

**Platform
Description** N/A

8.11 passive-interface

Use this command to disable the interface to send update packets. Use the **no** form of this command to enable the interface to send update packets.

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description	Parameter	Description
	default	Enables the passive mode on all interfaces.
	<i>interface-type interface-num</i>	Interface type and interface number.

Defaults No passive interface is configured by default.

Command mode Routing process configuration mode.

Usage Guide You can use the **passive-interface default** command to enable the passive mode on all interfaces. Then ,use the **no passive-interface interface-type interface-num** command to remove the specified interface from the passive mode.

Configuration Examples The following example shows how to enable the passive mode on all interfaces and remove interface ethernet 0/0 from the passive mode:

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface ethernet 0/0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.12 redistribute

Use this command to redistribute the route of other routing protocols to RIPng. Use the **no** form of this command to remove the redistribution configuration.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value* | **route-map** *route-map-name*]

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value* | **route-map** *route-map-name*]

**Parameter
Description**

Parameter	Description
bgp	Redistributes the BGP routes to RIPng.
connected	Redistributes the connected routes to RIPng.
isis [<i>area-tag</i>]	Redistributes the ISIS routes to RIPng. <i>area-tag</i> indicates the ISIS process number.
ospf <i>process-id</i>	Redistributes the OSPF routes to RIPng. <i>process-id</i> indicates the OSPF process number, and the range is from 1 to 65,535.
static	Redistributes the static routes to RIPng.
metric <i>metric-value</i>	(Optional) Sets the metric value for the route redistributed to RIPng.
route-map <i>route-map-name</i>	(Optional) Sets the redistribution route filtering.

Defaults

By default, the routes of other routing protocols are not redistributed.

If the **default-metric** command is not configured, the default metric value is 1;

By default, the **route-map** is not configured;

By default, all sub-type routes in the specified routing process are redistributed.

**Command
mode**

Routing process configuration mode.

Usage Guide

This command is used to redistribute the external routes to RIPng.

It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different. The RIP and OSPF metric calculations are incomparable for the reason that the RIP metric calculation is hop-based while the OSPF one is bandwidth-based.

The instance, from where the routing information is redistributed to the RIPng, must be specified in

the process of configuring the multi-instance protocol redistribution.

Configuration Examples The following example shows how to redistribute the static route, use the route map *mymap* to filter and set the metric value as 8:

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# redistribute static route-map
mymap metric 8
```

Related Commands

Command	Description
default-metric	Defines the default RIPng metric value when redistributing other routing protocols.
distribute-list	Filters the RIPng routing update packets.

Platform N/A

Description

8.13 show ipv6 rip

Use this command to show the parameters and each statistical information of the RIPng routing protocol process.

show ipv6 rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode or user mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show ipv6 rip
Routing Protocol is "RIPng"
Sending updates every 10 seconds with +/-50%, next due in 8 seconds
Timeout after 30 seconds, garbage collect after 60 seconds
Outgoing update filter list for all interface is:
distribute-list prefix aa out
Incoming update filter list for all interface is: not set
Default redistribution metric is 1
Default distance is 120
Redistribution:
  Redistributing protocol connected route-map rm
  Redistributing protocol static
  Redistributing protocol ospf 1
Default version control: send version 1, receive version 1
Interface          Send  Recv
VLAN 1              1     1
Loopback 1          1     1
Routing Information Sources:
None
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and each statistical information of the RIPng process.

Platform N/A

Description

8.14 show ipv6 rip database

Use this command to display the RIPng route entries.

show ipv6 rip database

Parameter Description

Parameter	Description
-----------	-------------

N/A	N/A
-----	-----

Defaults N/A

Command mode Privileged EXEC mode or user mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show ipv6 rip database
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP
sub-codes:n - normal,s - static,d - default,r - redistribute,
i - interface, a/s - aggregated/suppressed
S(r) 2001:db8:1::/64, metric 1, tag 0
Loopback 0/::
S(r) 2001:db8:2::/64, metric 1, tag 0
Loopback 0/::
C(r) 2001:db8:3::/64, metric 1, tag 0
VLAN 1/::
S(r) 2001:db8:4::/64, metric 1, tag 0
Null 0/::
C(i) 2001:db8:5::/64, metric 1, tag 0
Loopback 1/::
S(r) 2001:db8:6::/64, metric 1, tag 0
Null 0/::
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.15 split-horizon

Use the **split-horizon** command to enable the RIPng split-horizon function in routing process configuration mode. Use the **no** form of this command to disable this function. Use the **split-horizon poisoned-reverse** command to enable the RIPng poisoned reverse horizontal split function in routing process configuration mode. Use the **no** form of this command to disable this function.

split-horizon [poisoned-reverse]

no split-horizon [poisoned-reverse]

Parameter Description	Parameter	Description
	poisoned-reverse	(Optional) Enables the poisoned-reverse horizontal split.

Defaults RIPng split horizon is enabled by default.

Command mode Routing process configuration mode.

Usage Guide In the process of packet updating, split-horizon function prevents some routing information from being advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the **show ipv6 rip** command to determine whether the RIPng split-horizon function is enabled or not.

Configuration Examples The following example shows how to disable the RIPng horizontal split:

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# no split-horizon
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

8.16 timers

Use this command to adjust the RIPng timer. Use the **no** form of this command to restore the default settings.

timers *update invalid flush*

no timers

**Parameter
Description**

Parameter	Description
<i>update</i>	Sets the routing update time, in seconds. The update parameter defines the period of sending the routing update packets by the device. The invalid and flush parameter reset once the update packets are received.
<i>invalid</i>	Sets the routing invalid time, in seconds, starting from receiving the last valid update packet. The invalid parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
<i>flush</i>	Sets the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.

Defaults The default update time is 30 seconds; the default invalid time is 180 seconds; and the default flush time is 120 seconds.

Command mode Routing process configuration mode.

Usage Guide Adjusting the above time may speed up the RIPng convergence time and the troubleshooting time. The RIPng time must be consistent for the devices connecting to the same network. You are not

recommended to adjust the RIP time, except for the specific requirement.

Use the **show ipv6 rip** command to view the current RIPng time parameter setting.

In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.

Configuration The following example shows how to send the RIP update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds.

Examples

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# timers 10 30 90
```

**Related
Commands**

Command	Description
show ipv6 rip	Displays the parameters and the statistical information of the RIPng process.
show ipv6 rip database	Displays the RIPng routes.

Platform N/A
Description

9 NSM Commands

9.1 clear ip route

Use this command to clear the route cache.

```
clear ip route [ vrf vrf_name ] { * | network [ netmask ] | }
```

	Parameter	Description
Parameter Description	<i>vrf vrf_name</i>	(Optional) Specifies the route cache of the specified VRF instance. If no VRF is specified, the route cache of all VRF instances is cleared.
	*	Clears all route cache.
	<i>network</i>	Specifies the route cache of the network or subnet.
	<i>netmask</i>	(Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match <i>network</i> with the route. The cache of the longest match is cleared.

Command

Mode Privileged EXEC mode

Usage Clearing route cache clears the corresponding routes and triggers the routing protocol relearning.

Guide Please note that clearing all route cache leads to temporary network disconnection.

Examples The following example clears the cache of the route which is the longest match with IP address 192.168.12.0.

```
clear ip route 192.168.12.0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description

9.2 ip default-gateway

Use this command to configure the default gateway IP address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

```
ip default-gateway ip-address
```

```
no ip default-gateway
```

```
default ip default-gateway
```

Parameter	Parameter	Description
Description	<i>ip-address</i>	IPv4 address of the default gateway

Defaults No gateway IP address is configured by default.

Command

Mode Global configuration mode

Usage When the device does not know the destination address of a packet, the device will forward the packet to the default gateway.

Examples The following example sets the IP address of default gateway to 192.168.1.1.

```
ip default-gateway 192.168.1.1
```

Related	Command	Description
Commands	N/A	N/A

Platform

Description This command is supported on 2-layer devices.

9.3 ip default-network

Use this command to configure the default network globally. Use the **no** or **default** form of this command to restore the default setting.

ip default-network *network*

no ip default-network *network*

default ip default-network *network*

Parameter	Parameter	Description
Description	<i>network</i>	Default network

Defaults The default is 0.0.0.0/0.

Command

Mode Global configuration mode

Usage The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network.

Guide The default network always starts with an asterisk ("*"), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.

Examples

```
ip route 192.168.100.0 255.255.255.0 serial 0/1
ip default-network 192.168.100.0
```

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
ip default-network 200.200.200.0
```

Related**Commands**

Command	Description
show ip route	Displays the routing table.

9.4 ip fast-reroute route-map

Use this command to enable static fast reroute. Use the **no** or **default** form of this command to restore the default setting.

ip fast-reroute [vrf *vrf-name*] **static route-map** *route-map-name*

no ip fast-reroute [vrf *vrf-name*]

default ip fast-reroute [vrf *vrf-name*] **route-map**

Parameter**Description**

Parameter	Description
vrf <i>vrf-name</i>	VRF
route-map <i>route-map-name</i>	Route map
static	Backup route

Default

This function is disabled by default.

Command**Mode**

Global configuration mode

Usage**guideline**

Fast reroute provides an active next-hop and a backup one. If the active next-hop fails, the backup next-hop is used for forwarding.

To enhance the performance of fast reroute, enable the BFD detection function for the active next-hop. For interfaces that are up or down, to shorten the interruption time of fast reroute, configure **carrier-delay 0** in the interface configuration mode of the active outbound interface to optimize the performance.

For static fast reroute, if the active next-hop fails, the backup next-hop is used for forwarding.

Examples

The following example sets the backup next-hop of all static routes to 192.168.1.2 through the outbound interface of GigabitEthernet 0/1.

```
Ruijie(config)# route-map fast-reroute
Ruijie(config-route-map)# set fast-reroute backup-nexthop GigabitEthernet 0/1
192.168.1.2
Ruijie(config-route-map)# exit
Ruijie(config)# ip fast-reroute static route-map fast-reroute
```

Related	Command	Description
command	fast-reroute	Configures OSPF fast reroute.

Platform
Description

9.5 ip route

Use this command to configure a static route. Use the **no** or **default** form of this command to restore the default setting.

ip route [*vrf vrf_name*] *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent** | { **track** *object-number* | **arp** }] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**]

no ip route [*vrf vrf_name*] *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

no ip route [*vrf vrf_name*] **all**

default ip route [*vrf vrf_name*] *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

Parameter
Description

Parameter	Description
<i>vrf vrf_name</i>	Name of the VRF, which can be the single protocol IPv4 VRF or configured IPv4 address family multi-protocol VRF.
<i>network</i>	Network address of the destination
<i>net-mask</i>	Mask of the destination
<i>ip-address</i>	The next hop IP address of the static route
<i>interface</i>	(Optional) The next hop egress of the static route
<i>distance</i>	(Optional) The administrative distance of the static route
<i>tag</i>	(Optional) The tag of the static route
permanent	(Optional) Permanent route ID
track <i>object-number</i>	(Optional) Indicates correlation with Track. <i>object-number</i> indicates the ID of the track object. By default, the static route is not correlated with the Track function.
weight <i>number</i>	(Optional) Indicates the weight of the static route. The weight is 1 by default.
description <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of one to 60 characters.
disabled/enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
global	(Optional) Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by <i>vrf name</i> .
arp	(Optional) Indicates that the next hop belongs to a global

	VRF. By default, the VRF of the next hop is the same as the VRF specified by <i>vrf name</i> .
--	--

Defaults No static route is configured by default.

Command Mode Global configuration mode

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

You can specify the VRF that the static route belongs to. The default weight of the static route is 1. To view the static route of non default weight, execute the `show ip route weight` command. The parameter `weight` is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries. WCMP limit is generally 32 for routers. However, WCMP limit varies by switch models for their chipsets support different weights. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it. When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, `ip route 0.0.0.0 0.0.0.0 Fastethernet 0/0`. In this case, the switch may consider that all unknown destination networks are directly connected to the Fastethernet 0/0. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

Usage Guide

Association between a static route and a track object can be specified. When association between a static route and a specified track object is configured and the advertised track object status is inactive, the static route does not take effect. If the advertised track object status is active, the static route takes effect based on another status. With association between a static route and a track object, the third-party status concerned by the track object is mainly used to determine whether the static route takes effect. Association between a static route and a track object cannot be used for routes with the permanent attribute.

Association between a static route and an ARP object can be specified. When association between a static route and an ARP object is configured and the ARP object corresponding to the next hop and egress of the route does not exist, the static route does not take effect. When the ARP object corresponding to the next hop and egress of the route exists, the static route takes effect based on another status. Association between a static route and an ARP object cannot be used for routes with the permanent attribute.

Association between a static route and a track object cannot be used together with association between a static route and an ARP object.

Examples The following example adds a static route to the destination network of 172.16.100.0/24 whose next

hop is 192.168.12.1 and administrative distance is 15.

```
ip route 172.16.199.0 255.255.255.0 192.168.12.1 155
```

If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures data flows to be sent through fastethernet 0/0 to the destination network of 172.16.100.0/24.

```
ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1
```

Related Commands

9.6 ip route static bfd

Use this command to correlate the static route with BFD. Use the **no** or **default** form of this command to restore the default setting.

ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

no ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]


default ip route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

Use this command to correlate the static route with BFD. Use the **no** or **default** form of this command to restore the default setting.

Parameter	Description
vrf <i>vrf-name</i>	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
<i>interface-type interface-number</i>	Interface type and interface number.
gateway	Specifies the gateway IP address, that is, the BFD neighbor IP address. If the next hop of the static route is the neighbor, the BFD will detect whether this neighbor is reachable.
source <i>ip-address</i>	(Optional) The source IP address of the BFD session. If the neighbor device is multi hops away, you should specify the source IP address for the BFD session. No source IP address is specified by default.

Defaults The static address is not correlated with BFD by default.

Command Mode Global configuration mode

Usage Guide  Please make sure the BFD session parameters have been configured before executing this command.

Examples The following example correlates the static route with BFD, and detects the reachability of path to the

```

neighbor 172.16.0.2.
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport // No need to perform
this command on the router.
Ruijie(config-if-GigabitEthernet 0/1)# ip address 172.16.0.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# bfd interval 50 min_rx 50 multiplier
3
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)# ip route static bfd GigabitEthernet 0/1 172.16.0.2
Ruijie(config)# ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/1 172.16.0.2

```

Related**Commands** N/A**Platform****Description**

9.7 ip route static inter-vrf

Use this command to enable packets to be forwarded over VRF instances through the static route. Use the **no** or **default** form of this command to disable this function.

ip route static inter-vrf**no ip route static inter-vrf****default ip route static inter-vrf**

Use this command to enable packets to be forwarded over VRF instances through the static route. Use the **no** or **default** form of this command to disable this function.

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.**Command Mode** Global configuration mode

If the **no** form of this command is executed, packets are unable to be forwarded over VRF instances through the static route. If this command is executed and you want to use the **no** form of this command to disable such function, the following information will be displayed.

Usage Guide

```
*Aug 7 10:58:34: %NSM-6-ROUTESACROSSVRF: Un-installing route [x.x.x.x/8] from
global routing table with outgoing interface x/x.
```

Examples

The following example disables packets to be forwarded over VRF instances through the static route.

```
Ruijie(config)# no ip route static inter-vrf
```


**Related
Commands** N/A

**Platform
Description**

9.8 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** or **default** form of this command to disable this function.

ip routing
no ip routing
default ip routing

Defaults This function is enabled by default.

**Command
Mode** Global configuration mode

Usage Guide

IP routing is not necessary when the switch serves as bridge or VoIP gateway. When a device functions only as a bridge or VoIP gateway, the IP routing function of the RGOS software is not required. In this case, the IP routing function of the RGOS software can be disabled. After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the **no ip routing** command, the configuration of a large number of static routes may be lost. To prevent this situation, the static route configuration will be hidden temporarily when the **no ip routing** command is run. If the **ip routing** command is run again, the static route configuration can be restored.

Note that if the process or whole system restarts when the **no ip routing** command is run, the static route configuration will not be reserved.

Examples The following example disables IP routing.

```
Ruijie(config)# no ip routing
```

**Related
Commands** N/A

**Platform
Description**

9.9 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

ip static route-limit *number*

no ip static route-limit *number*

default ip static route-limit

	Parameter	Description
Parameter		
Description	<i>number</i>	Upper threshold of static routes in the range from 1 to 10000

Defaults The default is 1024.

Command Mode Global configuration mode

Usage Guide The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running-config** command.

Examples The following example sets the upper threshold of the static routes to 900 and then restores the setting to the default value.

```
ip static route-limit 900
```

Related Commands N/A

Platform Description

9.10 ipv6 default-gateway

Use this command to configure the default gateway IPv6 address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

ipv6 default-gateway *ipv6-address*

no ipv6 default-gateway

default ipv6 default-gateway

	Parameter	Description
Parameter		
Description	<i>ipv6-address</i>	Sets the default gateway IPv6 address.

Defaults	No gateway IPv6 address is configured by default.
Command Mode	Global configuration mode
Usage Guide	When the device does not know the destination address of a packet, the device will forward the packet to the default gateway. Use the command show ipv6 redirects to display default gateway configuration.
Examples	The following example sets the default gateway IPv6 address to 10::1. <pre>Ruijie(config)# ipv6 default-gateway 10::1</pre>
Platform Description	This command is not supported on 2-layer devices or 3-layer devices configured with the no ip routing command.

9.11 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** or **default** form of this command to restore the default setting.

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix / prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] [**tag** *tag*] [**weight** *number*] [**description** *description-text*]

no ipv6 route [**vrf** *vrf-name*] *ipv6-prefix / prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*]

no ipv6 route [**vrf** *vrf_name*] **all**

Parameter Description

Parameter	Description
vrf <i>vrf-name</i>	Name of VRF, which must be the configured IPv6 address family multi-protocol VRF
<i>prefix-length</i>	Mask length of the destination
<i>ipv6-address</i>	The next hop IP address of the static route
<i>interface</i>	(Optional) The next hop egress of the static route
nexthop-vrf <i>vrf-name1</i>	(Optional) VRF the nexthop belongs, which must be the configured IPv6 address family multi-protocol VRF.
<i>distance</i>	(Optional) The administrative distance of the static route. The default is 1.
<i>tag</i>	(Optional) The tag value of the static route. The default is 0.
weight <i>number</i>	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of

	these routes. The weight is 1 by default.
description <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of one to 60 characters.

Defaults No IPv6 static route is configured by default.

Command Mode Global configuration mode

When the multi-protocol VRF deletes the IPv6 address family, the IPv6 static route of VRF that the route or nexthop belongs is deleted.

If the VRF of the IPv6 static route interface is not same as the nexthop's VRF, then this IPv6 static route takes no effect.

Usage Guide The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115.

```
ipv6 route 2001::/64 2002::2 115
```

Examples If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastethernet 0/0 to the destination network of 2001::/64.

```
ipv6 route 2001::/64 fastethernet 0/0 2002::2
```

Related Commands	Command	Description
	show ipv6 route	Displays IPv6 routing table.

Platform Description

9.12 ipv6 route static bfd

Use this command to correlate the static route with BFD. Use the **no** or **default** form of this command to restore the default setting.

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

no ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

default ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ip-address*]

Parameter	Parameter	Description
-----------	-----------	-------------

Description	vrf <i>vrf-name</i>	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
	<i>interface-type interface-number</i>	Interface type and interface number.
	<i>gateway</i>	Specifies the gateway IP address, that is, the BFD neighbor IP address. If the next hop of the static route is the neighbor, the BFD will detect whether this neighbor is reachable.
	source <i>ipv6-address</i>	(Optional) The source IP address of the BFD session. If the neighbor device is multi hops away, you should specify the source IP address for the BFD session. No source IP address is specified by default.

Defaults The static route is not associated with BFD by default.

Command Mode Global configuration mode

Usage Guide  Please make sure the BFD session parameters have been configured before executing this command.

The following example correlates the static route with BFD, and detects the reachability of path to the neighbor `2001:1::2`.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# no switchport //
Ruijie(config-if)# ip address 2001:1::1/64
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)#exit
Ruijie(config)# ipv6 route static bfd GigabitEthernet 0/1 2001:1::2
Ruijie(config)# ipv6 route 2002::/64 GigabitEthernet 0/1 2001:1::2
```

Related Commands N/A

Platform Description

9.13 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

ipv6 static route-limit *number*

no ipv6 static route-limit *number*

default ipv6 static route-limit

Parameter	Parameter	Description
Description	<i>number</i>	Upper threshold of static routes in the range from 1 to 10000.
Defaults	The default is 1000.	
Command Mode	Global configuration mode	
Usage Guide	The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.	
Examples	The following example sets the upper threshold of the ipv6 static routes to 900 and then restores the setting to the default value.	
	<pre>Ruijie# ipv6 static route-limit 900 Ruijie# no ipv6 static route-limit</pre>	
Related Commands	Command	Description
	ipv6 route	Configures the IPv6 static route.
	show ipv6 route	Displays the IPv6 routing table.
Platform Description		

9.14 ipv6 unicast-routing

Use this command to enable the IPv6 route function of the RGOS. Use the **no** or **default** form of this command to disable this function.

ipv6 unicast-routing

no ipv6 unicast-routing

default ipv6 unicast-routing

Parameter	N/A
Description	
Defaults	This function is enabled by default.
Command Mode	Global configuration mode
Usage Guide	This function can be disabled if the device is just used as the bridge-connection device or the VOIP

gateway device.

Examples

The example disables the IPv6 route function of RGOS.

```
Ruijie# no ipv6 unicast-routing
```

Related Commands

Command	Description
ipv6 route	Configure the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table.

英文缺少

Platform

Description

9.15 maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** or **default** form of this command is used to restore the default setting.

maximum-paths *number*

no maximum-paths *number*

default maximum-paths

Parameter

Description

Parameter	Description
<i>number</i>	Number of equivalent routes in the range from 1 to 64

Defaults

It depends on switch models.


Command

Mode

Global configuration mode

The number of equivalent routes is configured to control the number of equivalent routes. After the number of equivalent routes is configured by running the **maximum-paths** command, the number of load-sharing channels in load-sharing mode will not exceed the number of configured static routes. You can run the **show running config** command to query the number of configured static routes. This command takes effect both to IPv4 and IPv6 addresses. After this command is configured, the maximum number of equivalent routes to an IPv4 or IPv6 destination is equal to the configured value.

Usage Guide

-  S8600/S5750/S7600 supports 64 groups of equivalent routes. Each group supports a maximum of 32 equivalent routes. The maximum number of equivalent routes on S3760/S5760 is 8. The number of static route groups is not restricted, that is, each route supports equivalent routes. An equivalent route group includes multiple equivalent next hops of the same prefix. On S8600/S5750/S7600, when 64 groups of equivalent routes are configured and an equivalent route needs to be configured for a prefix, the configuration is successful if the equivalent route exists in the 64 groups. Otherwise, the configuration fails.

The following example sets the number of equivalent routes to 10 and then restores the default setting.

Examples

```
maximum-paths 10
no maximum-paths 10
```

9.16 show ip redirects

Use this command to display the default gateway IP address.

show ip redirects

Use this command to display the default gateway IP address.

show ip redirects

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the default gateway IP address. This command is supported on 2-layer devices or 3-layer devices with the **no ip routing** command executed.

The following example displays the default gateway.

```
Ruijie# show ip redirects
Default Gateway: 192.168.195.1
```

Examples

Field	Description
Default Gateway	IP address of the default gateway.

Related Commands	Command	Description
	N/A	N/A

Platform Description

9.17 show ip route

Use the commands to display the configuration of the IP routing table.

show ip route [[*vrf vrf_name*] [*network* [*mask* [**longer-prefix**]] | **count** | *protocol* [*process-id*] | **weight**]]

show ip route [*vrf vrf-name*] [[**normal** | **ecmp** | **fast-reroute**]] [*network* [*mask*]]

Parameter	Parameter	Description
-----------	-----------	-------------

vrf vrf_name	(Optional) Displays the route information of the VRF.
<i>network</i>	(Optional) Displays the route information to the network.
<i>mask</i>	(Optional) Displays the route information to the network of this mask.
longer-prefix	(optional) Displays the routes that match the specified prefix.
count	(Optional) Displays the number of existent routes. (for the ECMP/WCMP route, displays one route)
<i>protocol</i>	(Optional) Displays the route information of specific protocol.
<i>process-id</i>	(Optional) Routing protocol process ID.
weight	(Optional) Displays the route information of non default weight.
normal	Displays normal routes and not equivalent routes or fast reroutes.
ecmp	Displays only equivalent routes.
fast-reroute	(Optional) Displays the master/standby route of fast reroute.

Defaults All routes are displayed by default.

Command Mode Privileged EXEC mode/ Global configuration mode/Interface configuration mode/ Routing protocol configuration mode/ Route map configuration mode

This command can display route information flexibly.

Usage Guide This command shows all routes. To show different attributes of routes, specify normal | ecmp | fast-reroute.

The following example displays the configuration of the IP routing table.

```
Ruijie# show ip route

Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default

Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
```

Examples

Field	Description
-------	-------------

O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Administrative distance/metric

```
Ruijie# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Field	Description
Routing Descriptor Blocks	Next hop IP address, source, update time, forwarding interface, source routing protocol and type of route information

```
Ruijie# show ip route count
----- route info -----
the num of active route: 5(include ecmp: 9)
```

```
Ruijie# show ip route weight
-----[distance/metric/weight]-----
S   23.0.0.0/8 [1/0/2] via 192.1.1.20
S   172.0.0.0/16 [1/0/4] via 192.0.0.1
```

```
Ruijie#show ip route normal
```

```
Codes: C - Connected, L - Local, S - Static
```

```
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       IA - Inter area, * - candidate default
```

```
Gateway of last resort is no set
```

```
S    20.0.0.0/8 is directly connected, VLAN 1
```

```
S    22.0.0.0/8 [1/0] via 20.0.0.1
```

```
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
```

```
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
```

```
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
```

```
C    192.1.1.0/24 is directly connected, VLAN 1
```

```
C    192.1.1.254/32 is local host
```

```
Ruijie#show ip route ecmp
```

```
Codes: C - Connected, L - Local, S - Static
```

```
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       IA - Inter area, * - candidate default
```

```
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
```

```
S*   0.0.0.0/0 [1/0] via 192.168.1.2
```

```
      [1/0] via 192.168.2.2
```

```
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
```

```
      [110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

```
Ruijie#show ip route fast-reroute
```

```
Codes: C - Connected, L - Local, S - Static
```

```
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       IA - Inter area, * - candidate default
```

```
Status codes: m - main entry, b - backup entry, a - active entry
```

```
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [ma] via 192.168.1.2
    [b] via 192.168.2.2
O IA 192.168.10.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1
    [ba] via 35.1.30.2, 00:38:26, VLAN 3
```

```
Ruijie# show ip route fast-reroute 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
[m] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
[ba]192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

9.18 show ip route static bfd

Use this command to display the IP route correlated BFD information

show ip route [[vrf vrf_name] static bfd

Use this command to display the IP route correlated BFD information

show ip route [[vrf vrf_name] static bfd

Parameter	Description
Description	vrf vrf-name (Optional) Displays route information of the specified VRF. The default is global VRF.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IP route correlated BFD information

The following example displays the IP route correlated BFD information,

```
Ruijie(config)#show ip route static bfd
S 10.0.0.0/8 via 100.100.100.25, GigabitEthernet 0/3, BFD state is Up
S 20.0.0.0/8 via 200.100.100.25, GigabitEthernet 0/4, BFD state is Admin
```

Examples

Field	Description
S	Static route
BFD state	State of the static route correlated BFD.

Related Commands N/A

Platform**Description**

9.19 show ip route summary

Use this command to display the statistical information about one routing table.

show ip route [vrf *vrf_name*] summary

Use this command to display the statistical information about all routing tables.

show ip route summary all

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name
Defaults	N/A	
Command		
Mode	Privileged EXEC mode	
Usage		
guideline	N/A	

The following example displays the statistics of the global routing table.

```
Ruijie# show ip route summary
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

Memory: 2000 bytes
Entries: 22,based on route prefixes
          NORMAL ECMP FRR TOTAL
Connected 3 0 0 3
Static 2 1 1 4
RIP 1 2 1 4
OSPF 2 1 1 4
ISIS 1 2 0 3
BGP 2 1 1 4
TOTAL 11 7 4 22
```

The following example displays the statistics of all routing tables.

```
Ruijie# show ip route summary all
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

IP routing table count:2
Total
Memory: 4000 bytes
Entries: 44,based on route prefixes
          NORMAL ECMP FRR TOTAL
Connected 6 0 0 6
Static 4 2 2 8
RIP 2 4 2 8
OSPF 4 2 2 8
ISIS 2 4 0 6
BGP 4 2 2 8
TOTAL 22 14 8 44

Global
Memory: 2000 bytes
Entries: 22,based on route prefixes
          NORMAL ECMP FRR TOTAL
Connected 3 0 0 3
Static 2 1 1 4
RIP 1 2 1 4
OSPF 2 1 1 4
ISIS 1 2 0 3
BGP 2 1 1 4
TOTAL 11 7 4 22
```

Examples

```

VRF1
Memory: 2000 bytes
  Entries: 22, based on route prefixes
  Entries: 29, based on route nexthops
NORMAL
ECMP FRR TOTAL
  Connected 3 0 0 3
  Static 2 1 1 4
  RIP 1 2 1 4
  OSPF 2 1 1 4
  ISIS 1 2 0 3
  BGP 2 1 1 4
  TOTAL 11 7 4 22

```

Field	Description
NORMAL	Type of the table entries. Value: NORMAL: common routes (not ECMP or FRR); ECMP: equivalent route; FRR: fast reroute; TOTAL: total
Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)
Connected	Protocol type. Value: Connected: direct connection; Static: static; RIP: RIP; OSPF: OSPF; ISIS: ISIS; BGP: BGP; TOTAL: total

9.20 show ip route track-table

Use this command to display the IP route correlated Track information.

show ip route [[vrf vrf_name] track-table

Use this command to display the IP route correlated Track information.

show ip route [[vrf vrf_name] track-table

Parameter	Parameter	Description
Description	vrf vrf_name	(Optional) Displays the route information of the specified VRF name. The default is global VRF,

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IP route correlated Track information.

The following example displays the IP route correlated Track information.

```
Ruijie(config)#show ip route track-table
ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/0 track 2 state is [up]
ip route 20.0.0.0 255.0.0.0 GigabitEthernet 0/0 2 track 3 state is [down]
```

Examples

:

Field	Description
track	Track target index
state	Track target state

Related Commands

Command	Description
N/A	N/A

Platform Description

9.21 show ipv6 redirects

Use this command to display the IPv6 default gateway IP address.

show ipv6 redirects

Use this command to display the IPv6 default gateway IP address.

show ipv6 redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

The following example displays the default gateway IPv6 address.

Examples

```
Ruijie# show ipv6 redirects
Default Gateway: 10::1
```


Field	Description
Default Gateway	IPv6 address of the default gateway

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

.

9.22 show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

```
show ipv6 route [ [ vrf vrf_name ] [ ipv6-prefix / prefix-length [ longer-prefixes ] | protocol [ process-id ] | weight ] ]
```

Use the command to display the configuration of the IPv6 routing table.

```
show ipv6 route [ [ vrf vrf_name ] [ ipv6-prefix / prefix-length [ longer-prefixes ] | protocol [ process-id ] | weight ] ]
```

Parameter	Description
vrf <i>vrf-name</i>	(Optional) Specifies a VRF.
<i>ipv6-prefix/prefix-length</i>	(Optional) Specifies a prefix for route's IPv6 address.
longer-prefixes	(Optional) Displays the route with an IPv6 address prefix mostly matched.
<i>protocol</i>	((Optional) Displays the route information of specific protocol.
<i>process-id</i>	(Optional) Specifies a route process ID.
weight	(Optional) Displays the non-default-weight routes only.

Defaults All routes are displayed by default.

Command

Mode Privileged EXEC mode

Usage Guide Use this command to display route information.

The following example displays the IPv6 routing table.

```
Ruijie(config)# show ipv6 route
```

Examples

```
IPv6 routing table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```

SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
IA - Inter area

C 10::/64 via Loopback 1, directly connected
L 10::1/128 via Loopback 1, local host
S 20::/64 [20/0] via 10::4, Loopback 1C
C FE80::/10 via Null 0, directly connected
C FE80::/64 via Loopback 1, directly connected
L FE80::2D0:F8FF:FE22:33AB/128 via Loopback 1, local host
    
```

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20::/64	Network address and mask of the destination network
[20/0]	Administrative distance/metric

Related Commands	Command	Description
	ipv6 route	Configures the IPv6 static route.

Platform Description

9.23 show ip route static bfd

Use this command to display the IPv6 route correlated BFD information

show ipv6 route [[vrf vrf_name] static bfd

Use this command to display the IPv6 route correlated BFD information

show ipv6 route [[vrf vrf_name] static bfd

Parameter	Description
Description	vrf vrf-name (Optional) Displays the route information of the designated VRF name of the static route. The default is global VRF,

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IPv6 route correlated BFD information.

The following example displays the IPv6 route correlated BFD information.

```
Ruijie(config)#show ip route static bfd
S    25::/64 via 100::25, GigabitEthernet 0/3, BFD state is Up
S    26::/64 via 200::25, GigabitEthernet 0/4, BFD state is Admin
```

Examples

Field	Description
S	Static route
BFD state	State of the static route associated BFD

Related Commands N/A

Platform Description

9.24 show ipv6 route summary

Use this command to display the statistics of the IPv6 routing table of a specified VRF.

show ipv6 route [vrf vrf-name] summary

Use this command to display statistics of all IPv6 routing tables.

show ipv6 route summary all

Parameter	Description
Description	vrf-name (Optional) VRF name. If no VRF name is specified, statistics of the IPv6 routing table of the global VRF are displayed.

	.
--	---

Defaults N/A

Command

Mode Privileged EXEC mode

Usage Guide N/A

The following example displays statistics of IPv6 routing table of the global VRF.

```
Ruijie#show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local          2
Connected      3
Static         0
PIP            0
OSPF           0
BGP            0
-----
Total          5
```

The following example displays t statistics of all IPv6 routing tables.

```
Ruijie#show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local          2
Connected      3
Static         0
PIP            0
OSPF           0
BGP            0
-----
Total          5
```

Examples

Field	Description
Memory	The memory size occupied by the current routing table.
Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field can be; Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry.

	OSPF: OSPF route entry. ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global (The default VRF) VRF1: VRF name. TOTAL: All VRF routing table summaries.

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

10 Protocol-independent Commands

10.1 accept-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its receiving direction. Use the no form of this command to restore the default value.

accept-lifetime *start-time* {**infinite** | *end-time* | **duration seconds**}

no accept-lifetime

Parameter description	Parameter	Description
	<i>start-time</i>	Start time of the lifetime. The syntax is as follows: <i>hh:mm:ss month date year</i> <i>hh:mm:ss date month year</i> <ul style="list-style-type: none"> ● hh—hour ● mm—minute ● ss—second ● month—month ● date—day ● year—year The default start time is Jun 1, 1993, which is also the earliest start time available.
	infinite	Indicates that the encryption key is valid for ever.
	<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
	duration seconds	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

Default infinite

Command mode Encryption key configuration mode

Usage guideline Use this command to specify the lifetime of an encryption key in its receiving direction.

Examples The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011.

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)#accept-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec
12 2011
```

Related

Command	Description
---------	-------------

command	-	-
----------------	---	---

Platform -
description

10.2 ip as-path access-list

Use this command to configure an autonomous system (AS) path filter using a regular expression. Use the **no** form of this command to remove the AS path filter using a regular expression.

ip as-path access-list *path-list-num* { **permit** | **deny** } *regular-expression*

no ip as-path access-list *path-list-num* [{ **permit** | **deny** } *regular-expression*]

Parameter description	Parameter	Description
	<i>path-list-num</i>	Specifies the AS-path access-list number. The range is from 1 to 500.
	permit	Permits advertisement based on matching conditions.
	deny	Denies advertisement based on matching conditions.
	<i>regular-expression</i>	Regular expression that defines the AS-path filter. The expression length range is from 1 to 255 characters.

Default By default, no AS path filter using a regular expression is configured.

Command mode Global configuration mode

Usage guideline N/A

Examples The following example configures an AS path filter matching the path which contains AS number 123 only.

```
Ruijie(config)# ip as-path access-list 105 deny ^123$
```

Related command	Command	Description
	-	-

Platform -
description

10.3 ip community-list

Use this command to define a standard or expanded community list and control access to it. Use the **no** form of this command to remove the setting.

```

ip community-list { community-list-number | standard community-list-name } { permit | deny }
[ { community-list-number | internet | local-AS | no-advertise | no-export } ]
ip community-list { community-list-number | expanded community-list-name } { permit | deny }
[ regular-expression ]

```

Parameter	Description
<i>community-list-name</i>	Name of the community list.
standard	Indicates standard community list numbered in 1 to 99.
expanded	Indicates expanded community list numbered in 100 to 199.
permit	Permits access to the community list.
deny	Denies access to the community list.
Parameter description <i>community-number</i>	<p>Community number in the form of AA:NN(AS number/2-byte numerical) in the range of 1 to 255 characters. It may also be one of the following value:</p> <p>Internet: Indicates the Internet community. All paths belong to this community.</p> <p>no-export: Indicates that this path will not be advertised to any EBGp peers.</p> <p>no-advertise: Indicates that this path will not be advertised to any BGP peers.</p> <p>local-as: Indicates that this path will not be advertised to out of the AS. When AS confederation is configured, this path will not be advertised to other ASs or sub-ASs.</p>

Default configuration None

Command mode Global configuration mode.

Usage guidelines This command is used to define the community list for BGP.

Examples

```

Ruijie(config)# ip community-list standard 1 deny 100.20.200.20
Ruijie(config)# ip community-list standard 1 permit internet

```

Related commands

Command	Description
match community	Match the community list.
set community-list delete	Remove the community value of the BGP path according to the community list.
show ip community-list	Show the community list information.

10.4 ip extcommunity-list

Use this command to create an extcommunity list and add an entry to the list. Use the **no** form of this command to remove the setting.

ip extcommunity-list {*expanded-list* | **expanded** *list-name* } { **permit** | **deny** } [*regular-expression*]

ip extcommunity-list {*standard-list* | **standard** *list-name* } { **permit** | **deny** } [*rt value*] [*soo value*]

Parameter	Description
<i>expand-list</i>	Indicates an extended extcommunity list, ranging from 100 to 199. One extcommunity list may contain multiple rules.
<i>standard-list</i>	Indicates a standard extcommunity list, ranging from 1 to 99. One extcommunity list may contain multiple rules.
expanded <i>list-name</i>	Indicates the name of an extended extcommunity, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
standard <i>list-name</i>	Indicates the name of a standard extcommunity list, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
permit	Defines an extcommunity rule for permitting.
deny	Defines an extcommunity rule for denying.
<i>regular-expression</i>	(optional) Defines a matching template that is used to match an extcommunity.
<i>sequence-number</i>	(Optional) Defines the sequence number of a rule, ranging from 1 to 2,147,483,647. If no sequence number is specified, the sequence number automatically increases by 10 when a rule is added by default. The initial number is 10.
rt	(Optional) Sets the RT attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended extcommunity configuration.
soo	(Optional) Sets the SOO attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended extcommunity configuration.
<i>value</i>	Indicates the value of an extended community (extend_community_value).

Parameter description

Default

It is disabled by default.

Command mode

Global configuration mode and ip extcommunity-list configuration mode.

Usage guidelines

This command is used to define the extcommunity list.

Examples

1.The following example defines an ip extcommunity-list.

```
Ruijie(config)# ip extcommunity-list 1 permit rt 100: 1
Ruijie(config)# ip extcommunity-list standard aaa permit rt
100: 2
Ruijie(config)# ip extcommunity-list expanded ext1 permit 200: [0~9][0~9]
```

2. The following example displays how to use ip extcommunity.

```
Ruijie(config)# route-map rt_in_filter
Ruijie(config-route-map)# match extcommunity 1
Ruijie(config-route-map)# match extcommunity ext1
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family vpn
Ruijie(config-router-af)#neighbor 3.3.3.3 send-community extended
Ruijie(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in
```

10.5 ip prefix-list

Use this command to create a prefix list or add an entry to the prefix list. Use the **no** form of this command to remove the prefix list or an entry.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix-length*]

no ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix-length*]

Parameter description

Parameter	Description
<i>prefix-list-name</i>	Name of the prefix list
<i>seq-number</i>	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry without a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
deny	Deny the route matching the prefix list.
permit	Permit the route matching the prefix list.
<i>ip-prefix</i>	Network address and mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and

“equivalent to”.

Default

configuration None

Command mode

Global configuration mode.

Usage guidelines

The ip prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching.

You can execute this command to define an exact match, or use “ge” or “le” to define a range match for a prefix for flexible configuration. “ge” indicates the range of minimum-prefix-length to 32; “le” indicates the range of the mask length of the IP prefix to maximum-prefix-length; “ge” and “le” indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix < minimum-prefix-length < maximum-prefix-length <=32.

Examples

The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24.

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre1 permit 201.1.1.0/24
Ruijie(config)# router ospf
Ruijie(config-router)# distribute-list prefix pre1 out rip
Ruijie(config-router)# end
```

10.6 ip prefix-list description

Use this command to add the description of a prefix list. Use the **no** form of this command to delete the description.

ip prefix-list *prefix-list-name* **description** *description-text*

Parameter description

Parameter	Description
<i>prefix-list-name</i>	Name of the prefix list
<i>description-text</i>	Description of the prefix list

Default

configuration No description is added for a prefix list, by default.

Command

mode Global configuration mode

The example below adds the description for the prefix list:

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description Deny routes from Net-A
```

10.7 ip prefix-list sequence-number

Use this command to enable sort function for a prefix list. Use the **no** form of this command to disable the sort function.

ip prefix-list sequence-number

Parameter**description**

Disabled

Default

configuration No sequence number is added for a prefix list, by default.

Command**mode**

Global configuration mode

The example below adds a sequence number for the prefix list:

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description deny routes from Net-A
```

Related**commands**

Command	Description
ip prefix-list	Configure the prefix list.

Platform**description**

N/A

10.8 ipv6 prefix-list

Use this command to create an IPv6 prefix list or add an entry in the prefix list. Use the **no** form of this command to delete an IPv6 prefix list or an entry in the prefix list.

ipv6 prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

no ipv6 prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

Parameter

Parameter	Description
-----------	-------------

<i>prefix-list-name</i>	Name of the prefix list
<i>seq-number</i>	Sequence number of an entry in the prefix list. Its range is 1 to 4294967294. If the sequence number is not specified in this command, the system will allocate a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one is the product of adding 5 to the sequence number of the proceeding entry.
permit	Permit the access to the matching result.
deny	Deny the access to the matching result.
<i>ipv6-prefix</i>	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: "ge" indicates the operation of "larger than" and "equivalent to".
<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: "le" indicates the operation of "less than" and "equivalent to".

Default

configuration No prefix list is created.

Command

mode Global configuration mode

The ipv6 prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching.

Usage guideline

You can execute this command to define an exact match, or use "ge" or "le" to define a range match for a prefix for flexible configuration. "ge" indicates the range of minimum-prefix-length to 128; "le" indicates the range of the mask length of the IP prefix to maximum-prefix-length; "ge" and "le" indicates the range of minimum-prefix-length to maximum-prefix-length, namely, ipv6-prefix mask length < minimum-prefix-length < maximum-prefix-length <= 128

The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 2222::/64.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre1 permit 2222::64
Ruijie(config)# ipv6 router ospf
Ruijie(config-router)# distribute-list prefix pre out rip
Ruijie(config-router)# end
```

10.9 ipv6 prefix-list description

Use this command to add the description of an IPv6 prefix list. Use the **no** form of this command to

delete the description.

ipv6 prefix-list *prefix-lis-name* **description** *description-text*

no ipv6 prefix-list *prefix-lis-name* **description** *description-text*

Parameter	Parameter	Description
description	<i>prefix-lis-name</i>	Name of the ipv6 prefix list
	<i>description-text</i>	Description of the ipv6 prefix list

Default

configuration No description is added for an IPv6 prefix list, by default.

Command

mode Global configuration mode

The example below adds the description for the prefix list:

Examples

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related commands

Command	Description
ipv6 prefix-list	Configure the IPv6 prefix list.

10.10 ipv6 prefix-list sequence-number

Use this command to enable the sorting function for an IPv6 prefix list. Use the **no** form of this command to remove the settings.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Parameter description

Disabled.

Default

configuration No sequence number is added for a prefix list, by default.

Command

mode Global configuration mode

The example below adds a sequence number for the prefix list:

Examples

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related

Command	Description
---------	-------------

commands	ipv6 prefix-list	Configure the IPv6 prefix list.
----------	------------------	---------------------------------

10.11 key

Use this command to define an encryption key and enter the encryption key chain configuration mode.

Use the no form of this command to delete it.

key *key-id*

no key *key-id*

Parameter	Parameter	Description
description	<i>key-id</i>	Key ID, ranging from 0 to 2147483647.

Default No encryption key is configured.

Command mode Encryption key chain configuration mode.

Usage guideline Use this command to define an encryption key.

Examples The following example configures encryption key chain ripkeys and key 1.

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
```

Related command	Command	Description
	-	-

Platform description -

10.12 key chain

Use this command to define a key chain and enter the key chain configuration mode. Use the no form of this command to delete it.

key chain *key-chain-name*

no key chain *key-chain-name*

Parameter	Parameter	Description
description	<i>key-chain-name</i>	Key chain name.

Default No key chain is configured.

Command mode Global configuration mode.

Usage guideline  For a key chain to take effect, you need to configure at least one key.

Examples The following example configures key chain ripkeys and enters the key chain configuration mode.

```
Ruijie(config)# key chain ripkeys
```

Related command	Command	Description
	-	-

Platform description -

10.13 key-string

Use this command to specify a key string. Use the no form of this command to delete it.

key-string [0|7] text

no key-string

Parameter description	Parameter	Description
	0	Use plaintext.
	7	Use encryption.
	<i>text</i>	Authentication string.

Default No key string is configured.

Command mode Encryption key configuration mode.

Usage guideline Use this command to specify a key string.

Examples The following example configures key chain ripkeys, key 1 and the key string abc:

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)#key-string abc
```

Related command	Command	Description
	-	-

Platform description -

10.14 match as-path

Use this command to redistribute the routes of AS_PATH attribute permitted by the access list in the route map configuration mode. Use the **no** form of this command to remove the setting.

match as-path *as-path-acl-list-num* [*as-path-acl-list-num.....*]

no match as-path *as-path-acl-list-num* [*as-path-acl-list-num.....*]

Parameter description	Parameter	Description
	<i>as-path-acl-list-num</i>	ACL number, in the range of 1 to 500.
	<i>access-list-name</i>	Name of the access list

Default configuration None.

Command mode Route map configuration mode.

The match as-path can be followed by an access list number or name.

Usage guidelines One or more match or set commands can be executed to configure one route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

```
Ruijie(config)# route-map ROUTEMAP2IBGP
Ruijie(config-route-map)# match as-path 20 30
```

Related commands

Command	Description
match community	Match the community.
match metric	Match the metric.
match origin	Match the source of routes.
set as-path prepend	Set the AS_PATH attribute of redistributed routes
set metric	Set the metric.
set metric-type	Set the metric type.

10.15 match community

Use this command to redistribute the routes matching the Community attribute permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match community { *community-list-number* | *community-list-name* } [**exact-match**]

[{ *community-list-number* | *community-list-name* } [**exact-match**] ...]

no match community { *community-list-number* | *community-list-name* } [**exact-match**]

[{ *community-list-number* | *community-list-name* } [**exact-match**] ...]

	Parameter	Description
Parameter description	<i>community-list-number</i>	Number of the standard community list in the range 1 to 99. Number of the extended community list in the range of 100 to 199
	<i>communitys-list-name</i>	Name of the community list in the range of less than 80 characters
	exact-match	Match the community list exactly.

Default configuration None.

Command mode Route map configuration mode.

The match community can be followed by more than one community list number or name, but the total of community lists and names should not be greater than 6.

Usage guidelines Each exact-match applies to only the previous list, not all the lists.

One or more match or set commands can be executed to configure one route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

```
Ruijie(config)# ip community-list 1 permit 100:2 100:30
Ruijie(config)# route-map set_lopref
Ruijie(config-route-map)# match community 1 exact-match
Ruijie(config-route-map)# set local-preference 20
```

	Command	Description
Related commands	match as-path	Match the AS_PATH attribute.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set metric-type	Set the metric type.

10.16 match extcommunity

Use this command to define the match rule for the BGP extcommunity. Use the no form of this command to cancel the setting.

match extcommunity { *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }

no match extcommunity { *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }

Parameter	Parameter	Description
-----------	-----------	-------------

description	<i>standard-list-number</i>	Standard extcommunity list number, ranging from 1 to 99. An extcommunity list may contains multiple excommunity values.
	<i>standard-list-name</i>	Standard excommunity name. An extcommunity list may contains multiple excommunity values.
	<i>expanded-list-num</i>	Expanded extcommunity list number, ranging from 100 to 199. An extcommunity list may contains multiple excommunity values.
	<i>expanded-list-name</i>	Expanded excommunity name. An extcommunity list may contains multiple excommunity values.

Default The rule is not defined in the associated route map.

Command mode Route map configuration mode.

Usage There are the following scenarios for a route map with an extcommunity:

guideline

1. The route map associated with **import map** uses the RT attribute to filter imported VRF routes.
2. The route maps associated with **neighbor route-map in** and **neighbor route-map out** are configured in the BGP VPNv4 address family mode and use the RT attribute to filter VPNv4 routes sent to or by BGP peers.

Examples 1. Define two extcommunity:

```
Ruijie(config)# ip extcommunity-list 1 permit rt 100: 1
Ruijie(config)# ip extcommunity-list 1 permit rt 100: 2
```

2. Define match rules in the route map:

```
Ruijie(config)# route-map rt
Ruijie(config-route-map)# match extcommunity 1
```

3. Use the route map.

```
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family vpnv4
Ruijie(config-router-af)# neighbor 3.3.3.3 route-map rt in
```

Related command	Command	Description
	ip extcommunity-list	Create an extcommunity list.
	show ip extcommunity-list	Show an extcommunity list.

Platform description -

10.17 match interface

Use **match interface** command to redistribute the routes whose next hop is the specified interface.

Use the **no** form of this command to remove the setting.

match interface *interface-type interface-number* [*...interface-type interface-number*]

no match interface [*interface-type interface-number* [...*interface-type interface-number*]]

Parameter description	Parameter	Description
	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface number

Default configuration None.

Command mode Route map configuration mode.

This command can be followed by multiple interfaces.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage guidelines For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol.

Examples

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match interface fastethernet 0/0
```

Related commands	Command	Description
	match ip address	Match the address in the access list.
	match ip next-hop	Match the next-hop IP address in the access list.
	match ip route-source	Match the source IP address in the access list.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.

set metric-type	Set the metric type.
set tag	Set the tag.

10.18 match ip address

Use **match ip address** command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the **no** form of this command to remove the setting.

match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}

no match ip address [*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]

	Parameter	Description
Parameter description	<i>access-list-number</i>	Number of the access list
	<i>access-list-name</i>	Name of the access list
	<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default configuration None.

Command mode Route map configuration mode.

Multiple access list numbers or names may follow match ip address.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage guidelines For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

Examples The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type-1 external type and the default metric being 40.

```
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
```

```

access-list 10 permit 200.168.23.0

route-map redrip permit 10
match ip address 10
set metric 40
set metric-type type-1!

```

Related commands

Command	Description
access-list	Set the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop address in the access list.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.19 match ip next-hop

Use **match ip next-hop** command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the **no** form of this command to remove the setting.

match ip next-hop {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}

no match ip next-hop [*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]

Parameter description

Parameter	Description
<i>access-list-number</i>	Number of the access list
<i>access-list-name</i>	Name of the access list
<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default

configuration None.

Command

mode Route map configuration mode.

Usage

Multiple access list numbers or names may follow match ip next-hop.

guidelines

You can redistribute the routes from one routing process to another routing process. For example,

you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 192.168.100.1
access-list 20 permit 172.16.10.1

route-map redrip permit 10
match ip next-hop 10 20
```

Examples

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.20 match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list. Use the **no** form of this command to remove the setting.

match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }

no match ip route-source [*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]

	Parameter	Description
Parameter description	<i>access-list-number</i>	Number of the access list
	<i>access-list-name</i>	Name of the access list
	<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default configuration None.

Command mode Route map configuration mode.

Multiple access list numbers may follow `match ip route-source`.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage guidelines For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more `match` or `set` commands can be executed to configure a route map. If the `match` command is not used, all the routes will be matched. If the `set` command is not used, no operation will be performed.

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the source IP address of the RIP route matches the access list 5, the OSPF allows for redistribution.

Examples

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 5 permit 192.168.100.1

route-map redrip permit 10
 match ip route-source
```

	Command	Description
Related commands	access-list	Set the access list.
	match ip address	Match the IP address in the access list.
	match interface	Match the next-hop interface of the route.
	match ip next-hop	Match the next-hop IP address in the access list.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.

set metric-type	Set the metric type.
set tag	Set the tag.

10.21 match ipv6 address

Use this command to redistribute the network routes permitted in the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 address { *access-list-name*] | **prefix-list** *prefix-list-name* }

no match ipv6 address

Parameter description	Parameter	Description
	<i>access-list-name</i>	Name of the access list.
	<i>prefix-list prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default configuration None

Command mode Route map configuration mode

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage guideline

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list v6acl, with the default metric being 30.

Examples

```
ipv6 router ospf
redistribute rip subnets route-map redrip
ipv6 access-list v6acl
10 permit ipv6 2620::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 30
```

Related commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 next-hop	Match the next-hop address in the IPv6 access list.
match ipv6 route-source	Match the route source address in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

10.22 match ipv6 next-hop

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 next-hop { *access-list-name* } | **prefix-list** *prefix-list-name*}

no match ipv6 next hop

Parameter description

Parameter	Description
<i>access-list-name</i>	Name of the IPv6 access list.
<i>prefix-list prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default

None

configuration**Command**

mode Route map configuration mode

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage**guideline**

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 40.

Examples

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 2620::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 40
```

**Related
commands**

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPV6 access list.
match ipv6 route-source	Match the route source address in the IPV6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

10.23 match ipv6 route-source

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 route-source { *access-list-name* } | **prefix-list** *prefix-list-name* }

no match ipv6 route-source

Parameter	Description
<i>access-list-name</i>	Name of the IPv6 access list.
<i>prefix-list prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default

configuration None

Command

mode Route map configuration mode

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage

guideline

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 50.

Examples

```
ipv6 router ospf
redistribute rip subnets route-map redrip

ipv6 access-list v6acl
10 permit ipv6 5200::64 any

route-map redrip permit 10
match ipv6 address v6acl
set metric 50
```

Related
commands

Command	Description
ipv6 access-list	Set the IPV6 access list.
match interface	Match the next-hop interface of the route.
match ipv6 address	Match the IP address in the IPv6 access list.
match ipv6 next-hop	Match the next hop in the IPv6 access list.
match metric	Match the route metric.
match route-type	Match the route type.
match tag	Match the route tag.
set metric	Set the metric for route redistribution.
set metric-type	Set the type for route redistribution.
set tag	Set the tag for route redistribution.

10.24 match metric

Use **match metric** command to redistribute the routes of the specified metric. Use the **no** form of this command to remove the setting.

match metric *metric*

no match metric *metric*

Parameter
description

Parameter	Description
<i>metric</i>	Route metric, in the range 0 to 4294967295

Default
configuration

None.

Command
mode

Route map configuration mode.

Usage
guidelines

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10.

Examples

```
router ospf 1
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
```

```
route-map redrip permit 10
match metric 10
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.25 match mpls-label

Use this command to specify the filtering conditions of a route map. When the BGP receives routes from its peers, only routes that meet the filtering conditions and have the required labels are accepted. Use the no form of this command to cancel this function.

match mpls-label

no match mpls-label

Parameter description

Parameter	Description
-	-

Default

If the associated route map does not define the rule, MPLS labels will not be required for receiving routes.

Command mode

Route map configuration mode.

Usage guideline

This command is used only for the route map associated with **neighbor route-map in**. It applies only to the receive direction. If this command is not included in the rules specified by the route map, then the MPLS labels will not be required for receiving routes.

This command does not apply to VPNv4 routes. It applies only to IPv4 routes with labels.

Examples

The following example creates a route map. Only routes that meet the following two conditions will be received.

1. The route prefix meets the acl1-defined rules.
2. The route includes MPLS labels.

```
Ruijie(config)# route-map infiltrer permit 10
Ruijie(config-route-map)# match ip address acl1
Ruijie(config-route-map)# match mpls-label
Ruijie(config-route-map)# exit
Ruijie(config)# router bgp 1
Ruijie(config-router)# neighbor 1.1.1.1 route-map infiltrer in
```

**Related
command**

Command	Description
neighbor send-label	Enable the function for the BGP and its peer to exchange routes with MPLS labels.
neighbor route-map out	Manage the policy for the BGP sending routes to its peers.
neighbor route-map in	Manage the policy for the BGP receiving routes from its peers.
set mpls-label	Assign an MPLS label to routes that meet the filtering conditions.

**Platform
description** -

10.26 match origin

Use this command to redistribute the routes whose source IP address is permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match origin {egp | igp | incomplete}

no match origin [egp | igp | incomplete]

**Parameter
description**

Parameter	Description
egp	Redistribute the routes from the remote EGP.
igp	Redistribute the routes from the local IGP.
incomplete	Redistribute the routes from an incomplete type.

**Default
configuration** None

**Command
mode** Route map configuration mode

**Usage
guideline** Use this command to set the origin of the routes to be redistributed. Only one origin can be set.

Examples

```
Ruijie(config)# route-map MY_MAP 10 permit
Ruijie(config-route-map)# match origin egp
Ruijie(config-route-map)# set community 109
Ruijie(config-route-map)# exit
Ruijie(config)# route-map MAP20 20 permit
Ruijie(config-route-map)# match origin incomplete
Ruijie(config-route-map)# set community no-export
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set origin	Set the source.

10.27 match route-type

Use this command to redistribute the network routes of the specified type. Use the **no** form of this command to delete the setting.

match route-type { **static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2** | **evpn-type-1** | **evpn-type-2** | **evpn-type-3** | **evpn-type-4** | **evpn-type-5** }

no match route-type [**static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**]

Parameter description

Parameter	Description
local	Indicates the local route type.
static	Indicates the static route type.
connect	Indicates the directly connected route type.
rip	Indicates the RIP route type.
internal	Indicates the OSPF internal route type.
external	Indicates the OSPF external route type.
type-1 type-2	Indicates the OSPF type-1 or type-2 route type.
level-1 level-2	Indicates the ISIS level-1 or level-2 route type.

Default

configuration None

Command

mode Route map configuration mode

Usage

You can redistribute the routing information from one routing process to another routing process. For

guideline example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain.

Examples

```
router rip
redistribute ospf route-map redrip
network 192.168.12.0

route-map redrip permit 10
match route-type internal
!
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the access list.
set tag	Match the IP address.

10.28 match tag

Use this command to redistribute the network routes with the specified tag. Use the **no** form of this command to delete the setting.

match tag *tag* [...*tag*]

no match tag [*tag* [...*tag*]]

Parameter description

Parameter	Description
<i>tag</i>	Route tag

Default**configuration** None**Command****mode** Route map configuration mode

Multiple tags may follow the match tag command.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage**guideline**

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain.

Examples

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute ospf 100 route-map redrip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match tag 50 80
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the next-hop IP interface.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match ip next-hop	Match the next-hop IP address.
match route-type	Match the route type.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.29 memory-lack exit-policy

Use this command to configure a policy to preferentially exit a routing protocol when the memory reaches the lower limit. Use the **no** form of this command to restore the default policy, namely, exit the

routing protocol which occupies the largest memory.

memory-lack exit-policy { **bgp** | **ospf** | **pim-sm** | **rip** }

no memory-lack exit-policy

Parameter description	Parameter	Description
	bgp	Preferentially exit BGP when the memory is insufficient.
	ospf	Preferentially exit OSPF when the memory is insufficient.
	pim-sm	Preferentially exit PIM-SM when the memory is insufficient.
	rip	Preferentially exit RIP when the memory is insufficient.

Default By default, the routing protocol which occupies the largest memory exits preferentially.

Command mode Global configuration mode

Usage guideline When the memory reaches the lower limit, you can disable a routing protocol to release the memory to ensure the normal running of other protocols.

When the system runs out of memory, disable a routing protocol which has the minimal impact on the system to ensure the operation of main services.

Configuring the policy to preferentially exit the routing protocols which are disabled cannot help the system release memory.

This command ensures the operation of main services to some extent when the memory is insufficient.

If the memory is further consumed, all routing protocols will exit and stop running.

Examples The following example configures a policy to preferentially exit the BGP protocol when the memory reaches the lower limit.

```
Ruijie(config)# memory-lack exit-policy bgp
```

Related command	Command	Description
	-	-

Platform description -

10.30 route-map

Use **route-map** to enter the route map configuration mode and define a route map. Use the **no** form of this command to remove the setting.

route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

no route-map *route-map-name* [{**permit** | **deny**}*sequence-number*]

Parameter	Parameter	Description
-----------	-----------	-------------

description	<i>route-map-name</i>	Name of the route map. The redistribute command references the route map according to its name. Multiple routing policies can be defined in a route map, and each policy corresponds to one sequence number.
	permit	(Optional) If the permit keyword is defined and the rule defined by match is met, The set command controls the redistributed routes. For policy-based routing, the set command controls the packet forwarding, and exits the route map operation. If the permit keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
	deny	(Optional) If the deny keyword is defined and the rule defined by match is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation. If the deny keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
	<i>sequence-number</i>	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

Default

configuration None.

Command

mode Global configuration mode.

At present, the RGOS software primarily uses the route map for route redistribution and policy-based routing.

1. Route redistribution control

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage guidelines

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

When you create the first route map policy, if *sequence-number* is not specified, it is 10 by default; If only one route map policy exists and *sequence-number* is not specified, no new route map policy will be created, and the existing route map policy will be accessed for configuration;

If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed.

2. policy-based routing

Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The match command defines packet filtering rule and the set command defines the action for the packets matching the filtering rules. The match command used includes match ip address and match length; the set command includes set ip tos, set ip precedence, set ip dscp, set ip [default] nexthop, set ip next-hop verify-availability, set [default] interface.

The following example enables the OSPF routing protocol to redistribute the RIP routes with the hop count of 4. In the OSPF route domain, the route type is the external route type-1, the default metric is 40 and the tag is 40.

Examples

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
!
route-map redrip permit 10
 match metric 4
 set metric 40
 set metric-type type-1
 set tag 40
```

Related commands

Command	Description
redistribute	Redistribute the routes.

10.31 send-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its send direction. Use the no form of this command to restore the default value.

send-lifetime *start-time* {infinite | *end-time* | **duration** *seconds*}

no send-lifetime

Parameter description

Parameter	Description
<i>start-time</i>	Start time of the lifetime.
infinite	Indicates that the encryption key is valid for ever.
<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
duration	Duration of the encryption key after the start time. The value ranges from 1 to

<i>seconds</i>	2147483646.
----------------	-------------

Default infinite

Command mode Encryption key configuration mode

Usage guideline Use this command to specify the lifetime of an encryption key in its send direction.

Examples The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)# send-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011
```

Related command	Command	Description
	-	-

Platform description -

10.32 set aggregator as

Use this command to specify the AS_PATH attribute for the aggregator of the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set aggregator as *as-number ip_addr*

no set aggregator as [*as-number ip_addr*]

Parameter description	Parameter	Description
	<i>as-number</i>	AS number of the aggregator.
	<i>ip_address</i>	IP address of the aggregator.

Default configuration None

Command mode Route map configuration mode

Usage guideline Use this command to set the AS_PATH attribute for the matched routes in the BGP routing domain. Only one group of parameters (as-number, ip-addr) is allowed to set at a time.

Examples

```
Ruijie(config)# route-map set-as-path
Ruijie(config-route-map)# match as-path 1
Ruijie(config-route-map)# set aggregator as 3 2.2.2.2
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the route metric.
match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

10.33 set as-path prepend

Use this command to specify the AS_PATH attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set as-path prepend *as-number*

no set as-path prepend

Parameter description

Parameter	Description
<i>as-number</i>	Indicates number of the AS_PATH attribute to be configured. The AS number ranges from 1 to 4294967295, and 1 to 65535.65535 in dot mode.

Default

configuration None

Command

mode Route map configuration mode

Usage**guideline**

Use this command to configure the AS_PATH attribute for the matched routes. Up to 10 ASs can be added into the as-path for one time.

Examples

```
Ruijie(config)# route-map set-as-path
Ruijie(config-route-map)# match as-path 1
Ruijie(config-route-map)# set as-path prepend 100 101 102
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.

match metric	Match the route metric.
match origin	Match the route source.
set community	Set the COMMUNITY attribute.
set metric	Set the metric.
set metric-type	Set the type.

10.34 set atomic-aggregate

Use this command to set the ATOMIC-AGGREGATE attribute for routes.

set atomic-aggregate

Use the **no** form of this command to delete existing configuration.

no set atomic-aggregate

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Routing map configuration mode	
Default Level	14	
Usage Guide	This command is used only in the BGP protocol and is used to set the ATOMIC-AGGREGATE attribute for routes.	
Configuration Examples	N/A	

10.35 set comm-list delete

Use this command to delete the COMMUNITY_LIST attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set comm-list *community-list-number* | *community-list-name* **delete**

no set comm-list *community-list-number* | *community-list-name* **delete**

Parameter description	Parameter	Description
	<i>community-list-number</i>	Number of the community list. Standard community list number : 1-99.

	Extended community list number : 100-199.
<i>community-list-name</i>	Name of the community list, which should be no more than 80 characters.

Default**configuration** None**Command****mode** Route map configuration mode**Usage****guideline** Use this command to set the community attribute value for the matched routes that will be deleted.**Examples**

```
Ruijie(config)# router bgp 100
Ruijie(config-router)# neighbor 172.16.233.33 remote-as 120
Ruijie(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPIN in
Ruijie(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out
Ruijie(config-router)# exit
Ruijie(config)# ip community-list 500 permit 100:10
Ruijie(config)# ip community-list 500 permit 100:20
Ruijie(config)# ip community-list 120 deny 100:50
Ruijie(config)# ip community-list 120 permit 100:.*
Ruijie(config)# route-map ROUTEMAPIN permit 10
Ruijie(config-route-map)# set comm-list 500 delete
Ruijie(config-route-map)# exit
Ruijie(config)# route-map ROUTEMAPOUT permit 10
Ruijie(config-route-map)# set comm-list 120 delete
```

**Related
commands**

Command	Description
match as-path	Match the AS_PATH attribute value.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set local-preference	Set the local priority of the route to be redistributed.
set metric-type	Set the metric type.

10.36 set community

Use this command to specify the community for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set community {*community-number*[*community-number...*] [**additive** | **none**]}

no set community

Parameter	Description
<i>community-number</i>	Community number in the form of AA:NN or a large numeral. In addition, it can be well-known community attributes like internet, local-AS, no-export and no-advertise.
additive	Increase on the original COMMUNITY attribute.
none	Set the community attribute as blank.

Default configuration None

Command mode Route map configuration mode

Usage guideline Use this command to set the community attribute for the matched route.

Examples

```
Ruijie(config)# route-map SET_COMMUNITY 10 permit
Ruijie(config-route-map)# match as-path 1
Ruijie(config-route-map)# set community 109:10
Ruijie(config-route-map)# exit
Ruijie(config)# route-map SET_COMMUNITY 20 permit
Ruijie(config-route-map)# match as-path 2
Ruijie(config-route-map)# set community no-export
```

Related commands

Command	Description
match as-path	Match the AS_PATH.
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set origin	Set the source.
set metric-type	Set the metric type.

10.37 set dampening

Use this command to specify the dampening parameters for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Parameter	Description
<i>half-life</i>	Half dampening life for the reachable or unreachable route in the range of 1 to 45 minutes, 15 minutes by default
<i>reuse</i>	When the route penalty is lower than this value, the route suppression is released. It is in the range 1 to 20000, 750 by default
<i>suppress</i>	When the route penalty is higher than this value, the route is suppressed. It is in the range 1 to 20000, 2000 by default
<i>max-suppress-time</i>	Maximum duration a route can be suppressed in the range 1 to 20000 minutes, 4* half-life by default.

Default configuration None

Command mode Route map configuration mode

Usage guideline Use this command to set the dampening parameter for the matched routes.

Examples

```
Ruijie(config)# route-map tag
Ruijie(config-route-map)# match as path 10
Ruijie(config-route-map)# set dampening 30 1500 10000 120
Ruijie(config-route-map)# exit
Ruijie(config)# router bgp 100
Ruijie(config-router)# neighbor 172.16.233.52 route-map tag in
```

Related commands

Command	Description
match as-path	Match the AS_PATH value.
match community	Match the community.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of the route to be redistributed.

10.38 set default interface

Use this command to specify the default interface for forwarding the packets whose route matches the rule but without an egress in the route map configuration mode. Use the **no** form of this command to remove the setting.

set default interface *interface-type interface-number* [...*interface-type interface-number*]
no set default interface *interface-type interface-number* [...*interface-type interface-number*]

	Parameter	Description
Parameter description	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

Default None

Command mode Route map configuration mode

Multiple interfaces may follow the set default interface command.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the device will determine how to process the packets to be routed according to the route map, which determines the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

If the first defined interface becomes down, the interface set by the second set command will be attempted. A route-map policy may contain multiple set operations.

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic whose packet size is less than 500 bytes and the route is not defined through fastEthernet 1/0 interface.

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# ip policy route-map smallpak
Ruijie(config-if)# exit
Ruijie(config)# route-map smallpak permit 10
Ruijie(config-route-map)# match length 0 500
Ruijie(config-route-map)# set default interface fastethernet 1/0
```

Examples

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
match length	Match the packet length.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets.
set ip precedence	Set the priority of the packets.

10.39 set extcommunity

Use this command to specify the extended COMMUNITY attribute for the routes that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set extcommunity {*rt* *extend-community-value* | **soo** *extend-community-value*}

no set extcommunity {*rt* | **soo** }

	Parameter	Description
Parameter description	rt	Specify the extended community value in the form of RT.
	soo	Specify the extended community value in the form of SOO.
	<i>extend-community-value</i>	Extended community value.

Default None

Command mode Route map configuration mode

Usage guideline Use this command to set the extended community attribute for the matched route.

Examples

```
Ruijie(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Ruijie(config)# route-map MAP_NAME permit 10
Ruijie(config-route-map)# match ip-address 2
Ruijie(config-route-map)# set extcommunity rt 100:2
```


	Command	Description
Related commands	match as-path	Match the AS_PATH value
	match community	Match the community.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set metric-type	Set the metric type.

10.40 set fast-reroute

Use this command to specify a backup outgoing fast reroute and a backup next-hop for routes that meet the match conditions. Use the **no** form of this command to delete the configuration.

set fast-reroute backup-interface *interface-type interface-number* [**backup-nexthop** *ip-address*]

no set fast-reroute

Parameter description	Parameter	Description
	<i>interface-type interface-number</i>	Backup outgoing interface.
	<i>ip-address</i>	Backup next-hop.
Default	-	
Command mode	Route map configuration mode.	
Usage guideline	<p>Use this command to configure IP FRR backup outgoing interface and backup next-hop. The current software version supports only one backup route. This command supports only one set of the two parameters.</p> <p>This command is used for fast reroute configuration.</p>	
	<p> IP FRR backup routes must not be direct-connection or local host routes.</p>	
Examples	<pre>Ruijie(config)# access-list 2 permit 192.168.78.0 255.255.255.0 Ruijie(config)# route-map frr permit 10 Ruijie(config-route-map)# match ip-address 2 Ruijie(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/1 backup-nexthop 192.168.1.2</pre>	
Related command	Command	Description
	match ip-address	Match IP address list.
Platform description	N/A	

10.41 set ip default next-hop

Use this command to specify the default next-hop IP address for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip default next-hop *ip-address* [*weight*] [...*ip-address* [*weight*]]

no set ip default next-hop [*ip-address* [*weight*] [...*ip-address* [*weight*]]]


Parameter description	Parameter	Description
	<i>ip-address</i>	IP address of the next hop.
	<i>weight</i>	Weight of the next hop.
Default configuration	None	
Command	Route map configuration mode	

mode

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight inputted.

Up to 32 IP addresses may follow the `set ip default next-hop` command.

If a weight follows ip address, up to 4 next hop IP addresses can be configured.

 If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

**Usage
guideline**

Differences between `set ip next-hop` and `set ip default next-hop`: After the `set ip next-hop` command is configured, the policy-based routing takes precedence over the routing table; while after the `set ip default next-hop` command is configured, the routing table takes precedence over the policy-based routing.

Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packet will be forwarded to the nexthop set with this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded through the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

The following example forwards the packets from two different nodes through different routes.

For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to device 6.6.6.6. For the messages received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to device 7.7.7.7. The other messages will be discarded if the software cannot find the forwarding route.

Examples

```
Ruijie(config)#access-list 1 permit 1.1.1.1 0.0.0.0
Ruijie(config)#access-list 2 permit 2.2.2.2 0.0.0.0
Ruijie(config)#interface async 1
Ruijie(config-if)#ip policy route-map equal-access
Ruijie(config)#route-map equal-access permit 10
Ruijie(config- route-map)#match ip address 1
Ruijie(config-route-map)#set ip default next-hop 6.6.6.6
Ruijie(config)#route-map equal-access permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip default next-hop 7.7.7.7
Ruijie(config)#route-map equal-access permit 30
Ruijie(config- route-map)#set default interface null 0
```

Related commands	Command	Description
	route-map	Define a route map.
	match ip address	Match the IP address.
	set default interface	Set the default outgoing interface.
	set interface	Set the outgoing interface.
	set ip next-hop	Set the next hop of the packets.
	set ip precedence	Set the priority of the packets.

Platform description N/A

10.42 set ip dscp

Use this command to specify the DSCP value for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip dscp *dscp-value*

no set ip dscp

Parameter description	Parameter	Description
		<i>dscp-value</i>

Default configuration N/A

Command mode Route map configuration mode

Usage guideline N/A

Examples N/A

Related commands	Command	Description
	route-map	Define a route map.
	match ip address	Match the IP address.
	set default interface	Set the default outgoing interface.
	set interface	Set the outgoing interface.
	set ip next-hop	Set the next hop of the packets.
	set ip precedence	Set the priority of the packets.

10.43 set ip next-hop

Use this command to specify the next-hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop *ip-address* [*weight*] [...*ip-address* [*weight*]]

no set ip] next-hop [*ip-address* [*weight*] [...*ip-address* [*weight*]]]


Parameter description	Parameter	Description
	<i>ip-address</i>	Indicates the next-hop IP address.
	<i>weight</i>	Indicates the weight of this next hop.

Default configuration None

Command mode Route map configuration mode

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32.

 If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

Usage guideline

If weight follows ip address, up to 4 next hop addresses can be configured.

This command can be used to set different routes for the traffic that meets different match rule. If multiple IP addresses are configured, they can be used in turn.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. After the policy-based routing is used, the device will decide how to process the packets that need be routed according to the route map, which decides the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

Examples

The following example enables policy-based routing on serial 1/0. When the interface receives the packets from 10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets

from 172.16.0.0/16, they will be sent to 172.16.100.1; all other packets will be discarded.

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#ip policy route-map load-balance
Ruijie(config)#access-list 10 permit 10.0.0.0 0.255.255.255
Ruijie(config)#access-list 20 permit 172.16.0.0 0.0.255.255
Ruijie(config)#route-map load-balance permit 10
Ruijie(config-route-map)#match ip address 10
Ruijie(config-route-map)#set ip next-hop 192.168.100.1
Ruijie(config)#route-map load-balance permit 20
Ruijie(config-route-map)#match ip address 20
Ruijie(config-route-map)#set ip next-hop 172.16.100.1
Ruijie(config)#route-map load-balance permit 30
Ruijie(config-route-map)#set interface Null 0
```

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

10.44 set ip next-hop verify-availability

Use this command to verify the availability of the next hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop verify-availability *ip-address* **track** *track-object-num*

no set ip next-hop verify-availability

Parameter description

Parameter	Description
<i>ip-address</i>	Indicates the next-hop IP address.
track	Judges whether the next hop is effective by using <i>Track</i> .
<i>track-object-num</i>	Indicates the track object number.
bfd	Indicates that BFD is used for neighbor detection.
<i>interface-type</i>	Configures the interface type.
<i>interface-number</i>	Configures the interface number.
<i>gateway</i>	Configures the gateway IP address, which is the neighbor IP address of BFD. If the next hop is configured as the neighbor, BFD will be

	used to detect the accessibility of the forwarding path.
--	--

Default

configuration None

Command

mode Route map configuration mode

Usage

guideline None

The following example verifies the availability of the next hop IP address being 192.168.1.2 and the number of the object to be tracked to 1.

Examples

```
Ruijie(config)#route-map rmap permit 10
Ruijie(config-route-map)#set ip next-hop verify-availability 192.168.1.2
track 1
```

**Related
commands**

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

10.45 set ip precedence

Use this command to set the precedence of the IP head of the packet matching the rule in the route map configuration mode. Use the **no** form of this command to remove the configured precedence setting.

set ip precedence {<0-7> | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ip precedence

**Parameter
Description**

Parameter	Description
<i>number</i>	Indicates the priority of the IP header with a number, ranging from 0 to 7. 7: critical 6: flash 5: flash-override 4: immediate

	3: internet 2: network 1: priority 0: routine
critical flash flash-override immediate internet network priority routine	Priority of an IP header.

Defaults N/A

Command mode Route map configuration mode

Usage guideline With different precedence values for the IP packet head configured, the IP packets matching the PBR routing are sent according to the different precedence values. Multiple set ip precedence commands can be executed in the route map configuration rule, but only the last one takes effect, and the precedence will be specified for the head of the IP packet matched the PBR.

The following example sets the precedence of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

Examples

```
Ruijie(config)#access-list 1 permit 192.168.217.68 0.0.0.0
Ruijie(config)#route-map name
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip precedence 4
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if)#ip policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip tos	Set the tos for the IP packet head.

10.46 set ip tos

Use this command to set the tos of the IP head of the packet matching the rule in the route map configuration mode. Use the **no** form of this command to remove the configured tos setting.

set ip tos {<0-15> | *max-reliability* | *max-throughput* | *min-delay* | *min-monetary-cost* | *normal*}

no set ip tos

Parameter Description	Parameter	Description
	<i>number</i>	Indicates the TOS value of an IP header with a number, ranging from 0 to 15. 2: max-reliability 4: max-throughput 8: min-delay 1: min-monetary-cost 0: normal
	max-reliability max-throughput min-delay min-monetary-cost normal	Priority of an IP header.

Defaults N/A

Command mode Route map configuration mode

Usage guideline With different TOS values for the IP packet head configured, the IP packets matching the PBR routing are transmitted with different service qualities.

The TOS value will be specified for the head of the IP packet matched the PBR.

The following example sets the TOS value of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

Examples

```
Ruijie(config)#access-list 1 permit 192.168.217.68 0.0.0.0
Ruijie(config)#route-map name
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip tos 4
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if)#ip policy route-map name
```

Related commands	Command	Description
	match interface	Match the next-hop interface.
	match ip address	Match the IP address in the ACL.

match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip precedence	Set the precedence for the IP packet head.

10.47 set ipv6 default next-hop

Use this command to specify the default next-hop IPv6 address for the IPv6 packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ipv6 default next-hop *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*] ...]

no set ipv6 default next-hop *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*] ...]

Parameter description

Parameter	Description
<i>global-ipv6-address</i>	Indicates the next-hop IPv6 address for packet forwarding. The next-hop router must be a neighbor router.
<i>weight</i>	Indicates the weight in the load balancing mode, ranging from 1 to 8. A larger value means larger packet traffic to be shared by the next hop.

Default

configuration None

Command

mode Route map configuration mode

With the policy-based routing applied to the interface, for the IPv6 packets matching the corresponding rules, if the usual route (that is the non default route) with the destination of this packet is not in the routing table, this packet will be forwarded to the next hop specified by the set ipv6 default next-hop command. Otherwise it is forwarded through the usual route. Noted that the match rule should be the IPv6 corresponded.

Usage

guideline




Packets select the egress from the policy-based routing and routing table in following priority.

set ipv6 next-hop;

usual route (the non default route)

set ipv6 default next-hop

default route.

-  For the switches, this function does not take effect if the mask length is beyond 64.
-  If this command and the `set ipv6 next-hop verify-availability` are both configured, the next hop set by the `set ipv6 next-hop verify-availability` command will take effect preferentially.
-  If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

The following example sets the default next hop of the packet with destination address `2001:0db8:2001:1760::/64` received at the interface `fastEthernet 0/0` as `2002:0db8:2003:1::95`

Examples

```
Ruijie(config)# ipv6 access-list acl_for_pbr
Ruijie(config-ipv6-acl)#permit ipv6 any 2001:0db8:2001:1760::/64
Ruijie(config)#route-map rm_if_0_0
Ruijie(config-route-map)#match ipv6 address acl_for_pbr
Ruijie(config-route-map)# set ipv6 default next-hop
2002:0db8:2003:1::95
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if)#ipv6 policy route-map rm_if_0_0
```

Related commands

Command	Description
<code>match ipv6 address</code>	Set the matching rule of policy-based routing.
<code>ipv6 policy route-map</code>	Use the policy-based routing on the interface.
<code>set ipv6 next-hop</code>	Set the next hop of the policy-based routing.

Platform description

N/A

10.48 set ipv6 next-hop

Use this command to specify the next-hop IPv6 address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ipv6 next-hop *global-ipv6-address* [weight] [...*global-ipv6-address* [weight]]

no set ip next-hop *global-ipv6-address* [weight] [...*global-ipv6-address* [weight]]

Parameter description

Parameter	Description
<i>global-ipv6-address</i>	IPv6 address of the next hop. The next hop router should be the neighbor router.
<i>weight</i>	Weight of the next hop in the load balancing mode, in the range of 1 to 8.

Default**configuration** None**Command****mode** Route map configuration mode


This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user.

Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32.

If weight follows ip address, up to 4 next hop addresses can be configured.

If the parameter vrf *vrf-name* is specified, packets forwarding will be across the VRF. The packets will be forwarded from VRF to public network with the parameter global specified. If no [vrf *vrf-name* | global] is specified, forwarding the IPv6 packets will inherit the VRF, that is the nexthop belongs to the VRF that receives this IPv6 packets.

Usage**guideline**

 If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

When the packets select the egress from the policy-based routing and routing table, the priorities are as follows.

```
set ipv6 next-hop;
usual route (the non default route)
set ipv6 default next-hop
Default route.
```

The following example sets the next hop of the packet with destination address *2001:0db8:2001:1760::/64* received at the interface *fastEthernet 0/0* as *2002:0db8:2003:1::95*

Examples

```
Ruijie(config)# ipv6 access-list acl_for_pbr
Ruijie(config-ipv6-acl)#permit ipv6 any 2001:0db8:2001:1760::/64
Ruijie(config)#route-map rm_if_0_0
Ruijie(config-route-map)#match ipv6 address acl_for_pbr
Ruijie(config-route-map)# set ipv6 next-hop
2002:0db8:2003:1::95
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if)#ipv6 policy route-map rm_if_0_0
```

Related commands

Command	Description
match ipv6 address	Set the matching rule of policy-based routing.
ipv6 policy route-map	Use the policy-based routing on the interface.

set ipv6 next-hop	Set the next hop of the policy-based routing.
--------------------------	---

Platform description	N/A
-----------------------------	-----

10.49 set ipv6 next-hop verify-availability

Use this command to determine the availability of the next-hop IP address.

set ipv6 next-hop verify-availability *global-ipv6-address* [**track** *track-obj-number* | **bfd** *interface-type interface-number gateway*]

Use the **no** form of this command to delete existing configuration.

no set ip next-hop verify-availability *global-ipv6-address* [**track** *track-obj-number* | **bfd** *interface-type interface-number gateway*]

Parameter Description

Parameter	Description
<i>global-ipv6-address</i>	Specifies the next-hop IPv6 address.
track	Detects whether the next hop is effective by using the tracking method.
<i>track-obj-number</i>	Specifies the tracking object number.
bfd	Conducts neighbor detection by using BFD.
<i>interface-type</i>	Specifies the interface type.
<i>interface-number</i>	Specifies the interface number.
<i>gateway</i>	Specifies the gateway IPv6 address, that is, IPv6 address of the BFD neighbor. If the configured next hop is the neighbor, the availability of the forwarding path will be detected using BFD.

Defaults	N/A
-----------------	-----

Command Mode	Routing map configuration mode
---------------------	--------------------------------

Default Level	14
----------------------	----

Usage Guide	This command is used only to configure PBR.
--------------------	---

Examples	The following example enables the PBR support for BFD and detects the forwarding path to the neighbor 2001:1::2 via BFD.
-----------------	--

```
Ruijie(config)# route-map rmap permit 10
Ruijie(config-route-map)# set ipv6 next-hop verify-availability 2001:1::2 bfd
FastEthernet 0/1 2001:1::2
```

10.50 set ipv6 precedence

Use this command to set the precedence of the IPv6 head of the packet matching the rule in the route map configuration mode. Use the **no** form of this command to remove the configured precedence setting.

set ipv6 precedence {<0-7> | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ipv6 precedence {<0-7> | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

	Parameter	Description
Parameter description	<i>critical</i> , <i>flash</i> , <i>flash-override</i> , <i>immediate</i> , <i>internet</i> , <i>network</i> , <i>priority</i> , <i>routine</i>	The precedence type of the IPv6 head.
	0~7	The configurable precedence range.

Default configuration N/A

Command mode Route map configuration mode

The following table shows the corresponding relationship between the value and type.

	Value	Type
Usage guideline	0	routing
	1	priority
	2	network
	3	internet
	4	immediate
	5	flash-override
	6	flash
	7	critical

The following example sets the precedence of IPv6 packet head as 3:

Configure the associated ACL6

```
Ruijie(config)#ipv6 access-list aaa
Ruijie(config-ipv6-acl)#permit ipv6 2003:1000::10/80 2001:100::/64
```

Configure route-map.

```
Ruijie(config)#route-map pbr-aaa permit 10
Ruijie(config-route-map)#set ipv6 next-hop 2001:1234::2
```

Modify the precedence.

```
Ruijie(config-route-map)# set ipv6 precedence 3
```

Or

Examples

```
Ruijie(config-route-map)# set ipv6 precedence immediate
```

	Command	Description
Related commands	match ipv6 address	Configure the ACL used for matching the packet in IPv6 PBR.
	route-map	Use the route map of the policy-based routing.
	set default interface	Set the default next-hop egress.
	set interface	Set the next hop egress.
	set ipv6 default next-hop	Set the default next-hop address for forwarding packets.
	set ipv6 next-hop	Set the next-hop address for forwarding packet.
	show ipv6 policy	Show the policy-based routing
	show route-map	Show the route map configuration.

Platform
description N/A

10.51 set level

Use this command to set the level of the area where the routes matching the rule are redistributed in the route map configuration command. Use the **no** form of this command to remove the setting.

set level {level-1 | level-2 | level-1-2 | stub-area | backbone}

no set level

Parameter description	Parameter	Description
	level-1	Indicates that the re-distribution route is advertised to ISIS Level 1.
	level-2	Indicates that the re-distribution route is advertised to ISIS Level 2.
	level-1-2	Indicates that the re-distribution route is advertised to ISIS Level 1 and Level 2.
	stub-area	Indicates that the re-distribution route is advertised to OSPF Stub Area.
	backbone	Indicates that the re-distribution route is advertised to the OSPF backbone area.

Default
configuration None

Command
mode Route map configuration mode

In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area.

Examples

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set level backbone
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

10.52 set local-preference

Use this command to set the **LOCAL_PREFERENCE** value for the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set local-preference *number*

no set local-preference

Parameter description

Parameter	Description
<i>number</i>	Local priority metric ranging 1 to 4294967295

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the local preference for the matched routes. Only one local preference can be set.

Examples

```
Ruijie(config)# route-map SET_PREF permit 10
Ruijie(config-route-map)# match as-path 1
Ruijie(config-route-map)# set local-preference 6800
Ruijie(config-route-map)# exit
Ruijie(config)# route-map SET_PREF permit 20
Ruijie(config-route-map)# match as-path 2
Ruijie(config-route-map)# set local-preference 50
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

10.53 set metric

Use **set metric** to set the metric for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric [+ *metric-value* | - *metric-value* | *metric-value*]

no set metric

Parameter description

Parameter	Description
+	Increase based on the metric of the original route
-	Decrease based on the metric of the original route
<i>metric-value</i>	Metric for the route to be redistributed

Default

configuration The default metric for route redistribution varies with the routing protocol.

Command

mode Route map configuration mode

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attention should be paid to the upper and lower limits of the routing protocols when you execute the `set metric`, `+ metric` or `- metric` commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more `match` or `set` commands can be executed to configure a route map. If the `match` command is not used, all the routes will be matched. If the `set` command is not used, no operation will be performed.

The following example enables the OSPF routing protocol to redistribute the RIP routes and sets the default metric to 40.

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set metric 40
```

Command	Description
<code>match interface</code>	Match the interface.
<code>match ip address</code>	Match the IP address.
<code>match ip next-hop</code>	Match the next-hop IP address.
<code>match ip route-source</code>	Match the source IP address.
<code>match metric</code>	Match the metric.
<code>match route-type</code>	Match the route type.
<code>match tag</code>	Match the tag.
<code>set metric-type</code>	Set the metric type.
<code>set tag</code>	Set the tag.

Usage guideline

Examples

Related commands

10.54 set metric-type

Use `set metric-type` to set the type of the routes to be redistributed. Use the `no` form of this command to remove the setting.

`set metric-type type`

`no set metric-type`

	Parameter	Description
Parameter description	<i>type</i>	Type of the routes to be redistributed. At present, you can set the type of the routes that the OSPF protocol redistributes. type-1: Type-1 external route; type-2: Type-2 external route.

Default configuration Type-2

Command mode Route map configuration mode

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage guideline

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.

Examples

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set metric-type type-1
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set tag	Set the tag.

10.55 set mpls-label

Use this command to enable the system to assign an MPLS label to routes that meet the filter condition of the route map when route updates are sent to BGP peers. Use the no form of this command to disable this function.

set mpls-label

no set mpls-label

Parameter description	Parameter	Description
	-	-

Default If the rule is not specified in the associated route map policy, MPLS labels will not be assigned to IPv4 routes sent to BGP peers.

Command mode Route map configuration mode.

Usage guideline This command applies only to the route map associated in **neighbor route-map out, which is used to manage the policy of the BGP for filtering IPv4 routes sent to its peers.**

This command takes effect only if you have used **neighbor send-label** to enable the BGP and its peers to exchange MPLS-labeled routes. Otherwise, routes will not be labeled. If this exchange function has been enabled but the associated route map does not configure **set mpls-label**, then routes that meet the filtering condition will be assigned only IPv4 routes and not an MPLS label.

Examples The following example creates a route map. The route prefixed with 1.1.1.1/32 is assigned an MPLS label. The one prefixed with 1.1.1.2/32 is assigned only a common IPv4 route update without a label. Routes that do not meet the rules defined by acl1 and acl2 will not send route updates to neighbors.

```
Ruijie (config)# ip access-list standard acl1
Ruijie (config-std-nacl) # permit host 1.1.1.1
Ruijie (config-std-nacl) # exit
Ruijie (config)# ip access-list standard acl2
Ruijie (config-std-nacl) # permit host 1.1.1.2
Ruijie (config-std-nacl) # exit
Ruijie (config)# route-map out-as permit 10
Ruijie (config-route-map)# match ip address acl1
Ruijie (config-route-map)# set mpls-label
Ruijie (config-route-map) # exit
Ruijie (config)# route-map out-as permit 20
Ruijie (config-route-map)# match ip address acl2
```

Related command	Command	Description
	neighbor send-label	Enable the function for the BGP and its peer to exchange routes with MPLS labels.
	neighbor route-map out	Manage the policy for the BGP sending route updates to its peers.

match mpls-label	Manage the policy for BGP peers receiving routes. Only routes with labels will be received.
show ip bgp labels	Show BGP-learned and BGP-sent routes with MPLS labels.

Platform description

-

10.56 set next-hop

Use this command to specify the next-hop IP address for the routes that match the rule. Use the **no** form of this command to remove the setting. This command is only used to configure routing policies.

set next-hop *ip-address*

no set next-hop

Parameter description	Parameter	Description
	<i>ip-address</i>	IP address of the next hop.

Default configuration None

Command mode Route map configuration mode

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

Usage guideline

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2.

Examples

```
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set next-hop 192.168.1.2
```

Related commands	Command	Description
	match interface	Match the interface.
	match ip address	Match the IP address.
	match ip next-hop	Match the next-hop IP address.

match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

10.57 set origin

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set origin {egp | igp | incomplete}

no set origin {egp | igp | incomplete}

Parameter description

Parameter	Description
egp	Redistribute the routes from the remote EGP.
igp	Redistribute the routes from the local IGP.
incomplete	Redistribute the routes from an unknown device.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Use this command to set the source of the routes to be matched. Only one route source attribute can be set.

Examples

```
Ruijie(config)# route-map SET_ORIGIN 10 permit
Ruijie(config-route-map)# match as-path 1
Ruijie(config-route-map)# set origin igp
Ruijie(config-route-map)# exit
Ruijie(config)# route-map SET_ORIGIN 20 permit
Ruijie(config-route-map)# match as-path 2
Ruijie(config-route-map)# set origin egp
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.

set local-preference	Set the local priority of redistributed routes.
-----------------------------	---

10.58 set originator-id

Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the **no** form of this command to remove the setting.

set originator-id *ip-addr*

no set originator-id [*ip-addr*]

Parameter	Parameter	Description
description	<i>ip-addr</i>	IP address of the originator.

Default configuration None

Command mode Route map configuration mode

Usage guideline Use this command to set the source of the routes to be matched.

Examples

```
Ruijie(config)# route-map SET_ORIGIN 10 permit
Ruijie(config-route-map)# match as-path 1
Ruijie(config-route-map)# set originator-id 5.5.5.5
Ruijie(config-route-map)# exit
Ruijie(config)# route-map SET_ORIGIN 20 permit
Ruijie(config-route-map)# match as-path 2
Ruijie(config-route-map)# set originator-id 5.5.5.6
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the route metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set local-preference	Set the local priority of redistributed routes.

10.59 set tag

Use this command to set the tag for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set tag *tag***no set tag**

Parameter	Parameter	Description
description	<i>tag</i>	Tag of the route to be redistributed

Default**configuration** The original routing tag remains unchanged.**Command****mode** Route map configuration mode**Usage****guideline** This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.

Examples

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set tag 100
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.

10.60 set weight

Use this command to set the weight for the BGP routes matching filtering rules. Use the **no** form of this command to remove the setting.

set weight *number***no set weight**

Parameter	Parameter	Description
description	<i>number</i>	Weight in the range of 0 to 65535

Default configuration None

Command mode Route map configuration mode

Usage guideline This command can only be used modify the weight of a BGP route.
By default, the weight of the route learned from a neighbor is the one configured with the neighbor weight command. The weight of the locally generated route is fixed 32768.

The following example sets the weight for the BGP route learned from the neighbor 1.1.1.1 at the inbound direction to 100.

Examples

```
Ruijie(config)# router bgp 1
Ruijie(config-router)# neighbor 1.1.1.1 route-map nei-rmap-in in
Ruijie(config-router)# exit
Ruijie(config)# route-map nei-rmap-in permit 10
Ruijie(config-route-map)# set weight 100
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match community	Match the route community.
match metric	Match the route metric.
match origin	Match the source.
set community	Set community of the redistributed route.
set metric	Set the metric of the redistributed route.
set metric type	Set the metric type of the redistributed route.

10.61 show ip as-path-access-list

Use this command to display the configuration of AS path access lists.

show ip as-path-access-list [*num*]

Parameter	Parameter	Description
description	<i>num</i>	AS path access list number.

Default N/A

Command Privileged EXEC mode

mode

Usage N/A
guideline

Examples The following example displays the AS path access lists.

```
Ruijie# show ip as-path-access-list
AS path access list 30
permit ^30$
```

Field	Description
AS path access list	AS path access list number
permit	Permits advertisement based on matching conditions.
^30\$	Regular expression.

Related
command

Command	Description
-	-

Platform
description

-

10.62 show ip community-list

Use **show ip community-list** command to display the community list.

show ip community-list [*community-list-number* | *community-list-name*]

Parameter
description

Parameter	Description
<i>community-list-number</i>	Number of the community list.
<i>community-list-name</i>	Name of the community list.

Default
configuration None

Command
mode Privileged EXEC mode

Usage
guidelines N/A

Examples

```
Ruijie# show ip community-list
Community-list standard local
permit local-AS
```

```
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

Related commands	Command	Description
	match community	Match the route community.
	set comm-list delete	Delete the community attribute in the BGP routes.

10.63 show ip extcommunity-list

Use this command to display the extcommunity list.

show ip extcommunity-list [*extcommunity-list-num* | *extcommunity-list-name*]

Parameter description	Parameter	Description
	<i>extcommunity-list-num</i>	extcommunity-list number, ranging from 1 to 199.
	<i>extcommunity-list-name</i>	extcommunity-list name.

Default -

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode and route map configuration mode.

Usage guideline -

Examples

```
Ruijie # show ip extcommunity-list
Standard extended community-list 1
 10 permit RT:1:200
 20 permit RT:1:100
Standard extended community-list 2
 10 permit RT:1:200
Expanded extended community-list rt_filter
 13 permit 1:100
```

Related command	Command	Description
	ip extcommunity-list	Create an extcommunity-list.
	match extcommunity	Match an extcommunity.
set extcommunity	Set an extcommunity.	

Platform description -

10.64 show ip prefix-list

Use **show ip prefix-list** to display the prefix list or the entries.

show ip prefix-list [*prefix-name*]

Parameter	Parameter	Description
description	<i>prefix-name</i>	Name of the prefix list.

Default

configuration The configuration information of all the prefix lists is displayed by default.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
Ruijie# show ip prefix-list
seq pre: 2 entries
seq 5 permit 192.168.564.0/24
seq 10 permit 192.2.2.0/24
```

10.65 show ip protocols

Use this command to display information about the status of the currently running IPv4 routing protocol.

show ip protocols [*vrf vrf-name*] { **bgp** | **isis** | **ospf** | **rip** }

Parameter Description	Parameter	Description
	<i>vrf-name</i>	Specifies the VRF instance name. If it is not specified, information about the status of routing protocols in global VRF mode is displayed.
	bgp	Displays information about the status of the BGP protocol.
	isis	Displays information about the status of the IS-IS protocol.
	ospf	Displays information about the status of the OSPF protocol.
	rip	Displays information about the status of the RIP protocol.
	-	Displays information about the status of all running routing protocols.

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and routing map configuration mode

Default Level 14

Usage Guide Information about the status of only the currently running routing protocol is displayed, and the information about a routing protocol that is not running is not displayed.

Examples The following example displays the status of routing protocols running in global VRF mode.

```
Ruijie# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 57.57.57.57
  Memory Overflow is enabled
  Router is not in overflow state now
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected, includes subnets in redistribution
    bgp, includes subnets in redistribution
  Number of areas in this router is 2: 2 normal 0 stub 0 nssa
  Routing for Networks:
    57.57.57.57 0.0.0.0 area 0
    163.18.4.0 0.0.0.255 area 0
    163.18.57.0 0.0.0.255 area 0
    192.100.1.0 0.0.0.255 area 0
    192.101.1.0 0.0.0.255 area 1
    192.102.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Distance: (default is 110)

Routing Protocol is "bgp 10"
  IGP synchronization is disabled
  Default-information originate is disabled
  Default local-preference applied to incoming route is 100
  Redistributing: connected
  Neighbor(s):
    Address          AddressFamily  FiltIn  FiltOut  DistIn  DistOut  RouteMapIn
RouteMapOut  Weight
  Distance: external 20(default) internal 200(default) local 200(default)
```

Field description:

Field	Description
Routing Protocol is "ospf 1"	Name of a routing protocol
Redistributing External Routes from	Route redistribution status of a routing protocol
Distance:	Distance information of a routing protocol

10.66 show ipv6 prefix-list

Use this command to display the information about the IPv6 prefix list or its entries.

show ipv6 prefix-list [*prefix-name*]

Parameter	Parameter	Description
description	<i>prefix-name</i>	Name of the IPv6 prefix list.

Default configuration The configuration information of all the IPv6 prefix lists is displayed.

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, route protocol configuration mode, route map configuration mode

Usage guideline If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
Ruijie# show ipv6 prefix-list
ipv6 prefix-list p6: 2 entries
    seq 5 permit 13::/20
    seq 10 permit 14::/20
```

10.67 show key chain

Use this command to display the key chain configuration.

show key chain [*key-chain-name*]

Parameter	Parameter	Description
description	<i>key-chain-name</i>	(Optional) Display the configuration of the specified key chain.

Default The configuration information of all key chains is displayed.

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and key chain configuration mode.

Usage guideline If no key chain is specified, the configuration information of all key chains is displayed.

Examples

```
Ruijie# show key chain
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
```

```
metric 10
Ruijie(config)#show key chain
key chain kc
  key 1 -- text "ruijie"
    accept-lifetime (12:11:00 May 2 2001) - (infinite)
    send-lifetime (always valid) - (always valid) [valid now]
```

Field	Description
key chain	Key chain name.
key	Key ID.
text	Key string.
accept-lifetime	Lifetime in the accept direction.
send-lifetime	Lifetime in the send direction.

Related command

Command	Description
-	-

Platform description

-

10.68 show route-map

Use the command to display the configuration of the route map.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
<i>route-map-name</i>	(Optional) Display the configuration information of the specified the route map.

Default configuration

The configuration information of all the route maps is displayed.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

Examples

```
Ruijie# show route-map
route-map AAA, permit, sequence 10
Match clauses:
```

```
ip address 2  
Set clauses:  
metric 10
```

Field	Description
route-map	Name of the route map.
Permit	The route map contains the permit keyword.
sequence 10	Sequence number of the route map.
Match clauses	Set the matching rule. Whether to perform the set operation depends on the permit or deny keyword in the route map.
Set clauses	Set the operation when the rule is matched.



Multicast Commands

1. IPv4 Multicast Routing Commands
2. IPv6 Multicast Routing Commands
3. IGMP Commands
4. MLD Commands
5. PIM-DM Commands
6. PIM-SM Commands
7. PIM-SMv6 Commands
8. IGMP Snooping Commands
9. MLD Snooping Commands

1 IPv4 Multicast Routing Commands

1.1 clear ip mroute

Use this command to remove the forwarding information of the IP multicast routes.

clear ip mroute { * | *group-address* [*source -address*] }

Parameter	Description
*	Remove all the forwarding information in the IP multicast route table.
<i>group-address</i>	Group IP address of IP multicast routes.
<i>source-address</i>	Source IP address of multicast routess.

Command Mode Privileged EXEC mode.

Examples The following example removes the entry whose group IP address is 230.0.0.1 from the multicast routing table:

```
Ruijie# clear ip mroute 230.0.0.1
```

Command	Description
show ip mroute	Show the forwarding information of multicast routes.

1.2 clear ip mroute statistics

Use this command to remove the statistics of IP multicast routes.

clear ip mroute statistics { * | *group-address* [*source -address*] }

Parameter	Description
*	Remove all the forwarding entries in the multicast route table.
<i>group-address</i>	Group IP address of IP multicast routes
<i>source-address</i>	Source IP address of multicast route.

Command Mode Privileged EXEC mode.

Usage Guide This command allows you to clear the statistics information of IP multicast routes.

Examples

The following example clears the statistics of entry with the group IP address 230.0.0.1 from the multicast routing table.

```
Ruijie# clear ip mroute statistics 230.0.0.1
```

Related Commands

Command	Description
show ip mroute	Show the multicast route forwarding information.
clear ip mroute	Clear the multicast route forwarding information.

1.3 ip mroute

Use this command to configure static multicast routes. Use the **no** form of this command to delete the configured routes.

ip mroute *source-address mask* [*protocol as-number*] {*rpf-address* | *interface-type interface-number*} [*distance*]

no ip mroute *source-address mask* [*protocol*]

Parameter Description

Parameter	Description
<i>source-address</i>	Source IP address of the multicast route
<i>mask</i>	Mask of the source IP address
<i>protocol</i>	(Optional) The unicast routing protocol being used.
<i>rpf-address</i>	Incoming interface of the multicast route
<i>interface-type</i> <i>interface-number</i>	Interface type and interface ID.
<i>distance</i>	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Default

distance: 0.

Command Mode

Global configuration mode.

Usage Guide

This command is used to configure the route for the purpose of RPF check. Note that the configured route is prior to the route learned in the unicast form.

Examples

The following example allows the multicast routes of all the sources in a network to pass 172.30.10.13:

```
Ruijie(config)# ip mroute 172.16.0.0 255.255.0.0
172.30.10.13
```

1.4 ip multicast boundary

Use this command to configure the boundary of an IP multicast group. The **no** form of this command removes the configured boundary.

ip multicast boundary *access-list*

no ip multicast boundary *access-list*

Parameter
Description

Parameter	Description
<i>access-list</i>	Access list associated with the multicast boundary.

Default

The boundary of a specified IP multicast group is defined by default.

Command Mode

Interface configuration mode

Usage Guide

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IP address.

Note:

This command filters IGMP and PIMSM packets of the specified IP address range. Multicast packets will not be received and sent through the interface of the boundary.

The following example configures svi1 as the boundary of all IP multicast groups.

Examples

```
Ruijie(config)# ip access-list mul-boun
Ruijie(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip multicast boundary mul-boun
```

1.5 ip multicast route-limit

Use this command to limit the number of the entries that can be added to the multicast routing table.

ip multicast route-limit *limit* [*threshold*]

no ip multicast route-limit *limit* [*threshold*]

Parameter
Description

Parameter	Description
<i>limit</i>	The number of the entries that can be added to the multicast routing table is 1 to 2147483647. The default value is 1024.
<i>threshold</i>	(Optional) Number of multicast routes at which alarms will be triggered. The default value is 2147483647.

Default The default value of *limit* is 1024.
The default value of *threshold* is 2147483647.

Command Mode Global configuration mode.

This command is used to restrict the number of route adding to the IPv6 multicast table. Note that the hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.

Usage Guide

For S86 and S12000, the default CPP value of PIM packets is 128pps and that of IGMP packets is 1000pps. Packets that exceed this value will be discarded.. If you want to use the PIM protocol to create more than 128 entries in the multicast routing table, you are advised to set the CPP value of PIM packets to the number of entries in the multicast routing table. If you want to use the IGMP protocol to create more than 1000 entries in the multicast routing table, you are advised to set the CPP value of IGMP packets to the number of entries in the multicast routing table.

Examples

The following example sets the route limit to 500.

```
Ruijie(config)# ip multicast route-limit 500
```

1.6 ip multicast rpf longest-match

Select the multicast static routing, MBGP routing and unicast routing that could be used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules.

Use this command to select the one with the mask longest-matched from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.

The no form of this command restores it to the default setting. By default, select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.

ip multicast rpf longest-match

no ip multicast rpf longest-match

Parameter
Description

Parameter	Description

Default

Select the multicast static routing, MBGP routing and unicast routing that are used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules. Then select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.

Command Mode Global configuration mode.

Examples The following example configures to select the routing with the longest-match.

```
Ruijie(config)# ip multicast rpf longest-match
```

1.7 ip multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. The **no** form of this command removes the setting.

ip multicast static *source-address group-address interface-type interface-number*

no ip multicast static *source-address group-address interface-type interface-number*

Parameter	Description
<i>source-address</i>	Source IP address
<i>group-address</i>	IP address of the multicast group
<i>interface-type interface number</i>	Layer 2 interface on which multicast packets are allowed to forward

Default Disabled

Command Mode Global configuration mode

You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces.

Usage Guide This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-DM or PIM-SM) may be affected because some features of the multicast protocol are driven by multicast flows.

The following example configures forwarding multicast flows (192.168.43.4 and 255.1.1.5) through GigabitEthernet 2/6 and FastEthernet 3/2.

Examples

```
Ruijie(config)# ip multicast static 192.168.43.4 225.1.1.5 G2/6
Ruijie(config)# ip multicast static 192.168.43.4 225.1.1.5 F3/2
```

1.8 ip multicast ttl-threshold

Use this command to configure TTL (time-to-live) threshold on the interface. Use the **no** form of the command to restore it to the default value.

ip multicast ttl-threshold *tvl-value*

ip multicast ttl-threshold

Parameter	Parameter	Description
Description	<i>tvl-value</i>	TTL threshold on the interface, within the range of 0 to 255.

Default The default *tvl-value* is 0.

Command Mode Interface configuration mode.

Usage Guide Use show running-config to display configuration. A device with multicast enabled can maintain one TTL threshold for every interface. If the TTL of the multicast packet received is greater than the threshold of the interface, the packets will be forwarded. Otherwise, the packet is discarded. Note that the TTL threshold is effective only to the multicast frames. In addition, you must configure it on the L3 interface.

Examples The following example sets the TTL threshold on the interface to 5.

```
Ruijie(config-if)# ip multicast ttl-threshold 5
```

1.9 ip multicast-routing

Use this command to enable multicast routing forwarding. The **no** form of this command disables multicast routing forwarding.

ip multicast-routing

no ip multicast-routing

Parameter	Parameter	Description
Description		.

Default Disabled.

Command Mode Global configuration mode.

This command allows you to enable IPv4 multicast routing forwarding. The multicast protocol will not be enabled with IPv4 multicast routing forwarding disabled.

Usage Guide

 It is not recommended to configure different v4 multicast routing protocols on different interfaces of a device.

Examples

This command enables multicast routing forwarding.

```
Ruijie(config)# ip multicast-routing
```

1.10 msf ipmc-overflow override

Use this command to enable the overflow overriding mechanism.

msf ipmc-overflow override

no msf ipmc-overflow override

Parameter	Parameter	Description
Description	-	-

Default Disabled.

Command Mode Global configuration mode.

Usage Guide N/A

The following example enables the overflow overriding mechanism.

Examples

```
Ruijie (config)# msf ipmc-overflow override
```

```
Ruijie (config)#
```

1.11 msf nsf

Use this command to configure the parameter for the continuous multicast forwarding.

msf nsf **{**{convergence-time *time*} | {leak *interval*} **}**

no msf nsf **{convergence-time | leak}**

Parameter	Parameter	Description
Description	convergence-time <i>ttl-value</i>	Maximum time for the multicast protocol convergence, in the valid range of the 0-3600s.
	leak <i>interval</i>	Packet multicast leak time, in the valid range of 0-3600s

Default convergence-time *time* :140s;
leak interval: 150s

Command Mode Global configuration mode.

Usage Guide N/A

The following example sets the maximum time for the protocol convergence.

```
Ruijie (config)# msf nsf convergence-time 300
Ruijie (config)#
```

Examples

The following example sets the packets leak time:

```
Ruijie(config)# msf nsf leak 200
Ruijie(config)#
```

1.12 show ip mrf mfc

Use this command to show the IPv4 multicast routing forwarding table.

show ip mrf mfc [*source-address group-address*]

Parameter	Description
<i>source-address</i>	Source address of the multicast routing forwarding entries.
<i>group-address</i>	Group address of the multicast routing forwarding entries.

Default All IPv4 multicast routing forwarding entries are displayed by default.

Command Mode Privileged EXEC mode.

The three parameters in this command are optional, wherein the source address and group address must be specified at the same time.

- Usage Guide**
- If no source address and group address are specified, all mfc entries are displayed.
 - When the source address and group address are specified only, the entries corresponding to the source and group addresses are displayed.

The following example shows all IPv4 layer-3 multicast routing forwarding entries with source address 20.0.1.30.

```
Ruijie#show ip mrf mfc 20.0.1.30 233.3.3.3
Multicast Routing and Forwarding Cache Table
(20.0.1.30, 233.3.3.3)
FAST_SW, SWTCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0
Incoming interface: VLAN 1[4097]
Outgoing interface list:
VLAN 3 (1)
```

Examples

The fields in the execution of the **show ip mrf mfc** command are described in the following table.

Field	Description
20.0.1.30	Source address of the entry.
233.3.3.3	Group address of the entry.
FAST_SW	The Flag shows whether to allow the fast forwarding or not. If the non-Ethernet interface, ppp, hdlc and frame relay exist, no fast forwarding entry generates.
SWTCHED	Indicate whether the entry configuration on the next layer forwarding table has done not not.
MIN_MTU MTU	The minimum MTU of the entry.
MIN_MTU_IFINDEX	The interface index with the minimum MTU value.
WRONG IF	The statistics number of the multicast data packets received on the wrong incoming interface.
Incoming interface	Incoming interface of the entry.
VLAN 3 (1)	The layer-3 outgoing interface of the entry is VLAN3. 1 for the ttl threshold of this layer-3 interface.

1.13 show ip mroute

Use this command to show the multicast forwarding table.

show ip mroute [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]

**Parameter
Description**

Parameter	Description
<i>group-address</i>	Multicat group IP address
<i>group-or-source-address</i>	Multicast or source IP address
<i>group-or-source-address</i>	Multicast or source IP address. The two addresses must not be the multicast addresses or source addresses at the samet time.
dense	Show PIM-DM multicast routing table.
sparse	Show PIM-SM multicast routing table.
summary	Show the summary of the multicast routing table.
count	Show the count of the multicast routing table.

Command Mode Privileged EXEC mode.

Examples The following example shows the information of the multicast routing table:

```
Ruijie# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example shows the information of a specific entry:

```
Ruijie# show ip mroute 10.10.1.52 224.0.1.3
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
Owner PIM-SM, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example shows the count of the routing table:

```
Ruijie# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT rcv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK rcv/Reg NACK rcv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT rcv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example shows the summary of the routing table:

```
Ruijie# show ip mroute summary
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
```

```
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: T
```

Field	Description
Flags	I-Immediate statistic T-Timed statistic F-Already set to the forwarding table
Timers:Uptime/Stat Expiry	Time when the entry is created. Time when it is aged.
Interface State	Interface state.
Owner	Owner of the entry, which may be a multicast routing protocol
Incoming interface	Expected packet incoming interface. If the actual incoming interface does not match it, the packets will be discarded.
Outgoing interface list	Outgoing interface list; the packets will be forwarded on the interfaces in the list.
Forwarding Counts: Pkt count/Byte count,	Forwarding count: packet count/byte count forwarded by the entry
Other Counts: Wrong If pkts	Count of the packets received from the wrong incoming interface.

Related Commands

Command	Description
ip multicast-routing	Enabling the multicast routing forwarding.
ip pim dense-mode	Enable the PIM-DM on the interface.
ip pim sparse-mode	Enable the PIM-SM on the interface.

1.14 show ip mroute static

Use this command to show the v4 static multicast routing information.

show ip mroute static

Parameter

Description

Parameter	Description

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to show the user-configured static multicast routing. In the same conditions, the priority of the static multicast routing is higher than the dynamically learned.

The following example shows the information of the user-configured static multicast routing:

Examples

```
Ruijie#show ip mroute static
Mroute: 172.16.0.0, RPF neighbor: 172.30.10.13
Protocol: , distance: 0
```

1.15 show ip mvif

Use this command to show the basic information of the multicast interface.

show ip mvif { *interface-type interface-number* }

Parameter**Description**

Parameter	Description
<i>interface-type interface-number</i>	Interface Type and number

Command Mode

Privileged EXEC mode.

The following example shows the basic information of the multicast interface of svil.

Examples

```
Ruijie#show ip mvif vlan 1
Interface Vif Owner TTL Local Remote Uptime
Idx Module Address Address
VLAN 1 1 PIM-DM 2 192.168.1.1 0.0.0.0 00:13:16
```

1.16 show ip rpf

Use this command to show the RPF information of the specified source IP address.

show ip rpf {*source-address* [*group-address*] [*rd route-distinguisher*]} [**metric**].

Parameter**Description**

Parameter	Description
<i>source-address</i>	Specified source IP address
<i>group-address</i>	Specified source IP address
<i>rd route-distinguisher</i>	Use the RD proxy for the searching.
metric	Show the metric of the MDT-SAFI route.

Command Mode

Privileged EXEC mode.

The following example shows the information of the RPF to 192.168.1.54:

Examples

```
Ruijie# show ip rpf 192.168.1.54
RPF information for 192.168.1.54
RPF interface: VLAN 1
RPF neighbor: 0.0.0.0
```

```

RPF route: 192.168.1.0/24
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0 RPF information for 192.168.1.54
RPF interface: VLAN 1
RPF neighbor: 0.0.0.0
RPF route: 192.168.1.0/24
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0

```

1.17 show msf msc

Use this command to show IPv4 multi-layer multicast forwarding table.

show msf msc [*source-address*] [*group-address*] [*vlan-id*]

Parameter	Description
<i>source-address</i>	Specified source IP address of the multi-layer multicast forwarding table.
<i>group-address</i>	Specified group address of the multi-layer multicast forwarding table.
<i>vlan-id</i>	The Vlan id where the incoming interface of the multi-layer multicast forwarding table is. 4096 indicates a routed port.

Default All IPv4 multi-layer multicast forwarding entries are displayed by default.

Command

Mode Privileged EXEC mode.

The three parameters in this command are optional.

If no source address and group address are specified, all mfc entries are displayed.

Usage Guide

- If only the source address is specified as s1, all msc entries with source address 1 are displayed.
- If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed.
- If the source address is specified as s1, the group address as g1 and the vlan id as v1, all corresponding msc entries are displayed.
- Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.

Examples The following example shows the IPv4 layer-3 multicast forwarding entries with source IP

address 192.168.195.25:

```
Ruijie# show msf msc 192.168.195.25
Multicast Switching Cache Table
(192.168.195.23, 233.3.3.3, 1), SYNC, MTU:0, 1 OIFs
VLAN 1(0): 1 OPORTs, REQ: DONE
OPORT 6, IGMP-SNP, REQ: DONE
```

The fields in the execution of the **show mrf mfc** command are described in the following table.

Field	Description
192.168.195.23	Source address of the entry.
233.3.3.3	Group address of the entry.
1	Vlan id where the incoming interface of the entry is.
SYNC	The entry has been synchronized to the hardware.
MTU	MTU value
OIFs	Layer-3 outgoing interface number.
VLAN1(0)	The vlan where the layer-3 outgoing interface oif is.
1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.
REQ: DONE	This oif configuration on the hardware has done.
OPORT 6	The layer-2 port in the oif with index 6.
IGMP-SNP	This port is created by the IGMP SNOOPING protocol. This value can also be the PIM-SNP, which means this port is created by the PIM SNOOPING protocol. And the ROUTER means this port is created by the layer-3 protocol.
REQ: DONE	The port configuration on the hardware has done.

1.18 show msf nsf

Use this command to show the configuration of continuous multicast forwarding.

show msf nsf

Parameter
Description

Parameter	Description
-	-

Command Mode

Privileged EXEC mode.

Examples

The following example shows the configuration of continuous multicast forwarding.

```
Ruijie# show msf nsf
Multicast HA Parameters
-----+-----
protocol convergence timeout 120 secs
flow leak interval 20 secs
```

```
Ruijie#
```

Related Commands

Command	Description
msf nsf	Configure the multicast NSF parameter.

2 IPv6 Multicast Routing Commands

2.1 clear ipv6 mroute

Use this command to remove the specific or all IPv6 multicast forwarding entries.

clear ipv6 mroute { * | *v6group-address* [*v6source -address*]

Parameter	Description
*	Removes all the forwarding information in the IPv6 multicast route table.
<i>v6group-address</i>	Group IPv6 address of IPv6 multicast routes
<i>v6source-address</i>	Source IPv6 address of multicast routes

Command Mode Privileged EXEC mode

Configuration The following example removes all the multicast routing entries.

Examples Ruijie# clear ip mroute *

Command	Description
show ipv6 mroute	N/A
clear ipv6 mroute statistics	N/A

2.2 clear ipv6 mroute statistics

Use this command to remove the statistics of IPv6 multicast routes.

clear ipv6 mroute statistics { * | *v6group-address* [*v6source -address*]

Parameter	Description
*	Removes all the forwarding entries in the multicast route table.
<i>v6group-address</i>	Group IPv6 address of IPv6 multicast routes
<i>v6source-address</i>	Source IPv6 address of multicast route

Command Mode Privileged EXEC mode

Usage Guide This command allows you to clear the statistics information of IPv6 multicast routes.

Configuration The following example clears all the statistical information of the multicast routing entries.

Examples Ruijie# clear ip mroute statistics *

Related Commands	Command	Description
	<code>show ipv6 mroute</code>	Displays the multicast route forwarding information.
	<code>clear ipv6 mroute</code>	Clears the multicast route forwarding information.

2.3 ipv6 mroute

Use this command to configure static IPv6 multicast routes. Use the **no** form of this command to restore the default setting.

ipv6 mroute *ipv6-prefix/prefix-length* [*protocol as-number*] { *v6rpf-address* | *interface-type interface-number* } [*distance*]

no ipv6 mroute *ipv6-prefix/prefix-length* [*protocol as-number*] { *v6rpf-address* | *interface-type interface-number* } [*distance*]

Parameter Description	Parameter	Description
	<i>ipv6-prefix/prefix-length</i>	Source IPv6 address of the multicast route
	<i>mask</i>	Mask of the source IPv6 address
	<i>protocol</i>	(Optional) The unicast routing protocol being used
	<i>v6rpf-address</i>	Incoming interface of the multicast route
	<i>interface-type</i> <i>interface-number</i>	Interface type and interface ID
	<i>distance</i>	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Defaults The static IPv6 multicast routing is not configured by default.

Command Mode Global configuration mode

This command is used to configure the route for the purpose of RPF check. Note that the configured route is prior to the route learned in the unicast form.

If the outgoing direction of static multicast route but not the next-hop IP shall be specified, the outgoing direction must be of the point-to-point type.

Usage Guide

The RPF rule is that when a best multicast route from the multicast list is selected, if the BGP multicast route and the static multicast route coexist, the latter one takes the precedence; select a best unicast route from the unicast list and compare the mask length of the best multicast and unicast routes, the one with greater mask length becomes the RPF route; if both mask length are the same, you shall compare the distance, and the one with smaller distance becomes the RPF route; if both distance values are the same, the multicast route becomes the RPF route.

Configuration Examples The following example allows the static multicast route 2233::/64 to pass 3333::3333:

```
Ruijie(config)# ipv6 mroute 2233::/64 3333::3333
```

2.4 ipv6 multicast boundary

Use this command to configure the boundary of an IPv6 multicast group. Use the **no** form of this command to restore the default setting.

ipv6 multicast boundary *access-list-name*

no ipv6 multicast boundary *access-list-name*


Parameter	Parameter	Description
Description	<i>access-list-name</i>	Access list associated with the multicast boundary

Defaults The boundary of a specified IPv6 multicast group is not defined by default.

Command Mode Interface configuration mode

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IPv6 address.

Usage Guide

 This command filters MLD, PIM-SMv6 packets of the specified IPv6 address range. Multicast packets will not be received and sent through the interface of the boundary.

The following example configures svi1 as the boundary of all IPv6 multicast groups.

```
Ruijie(config)# ip access-list mul-boun
Ruijie(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip multicast boundary mul-boun
```

Configuration Examples

2.5 ipv6 multicast route-limit

Use this command to limit the number of the entries that can be added to the IPv6 multicast routing table. Use the **no** form of this command to restore the default setting.

ipv6 multicast route-limit *limit* [*threshold*]

no ipv6 multicast route-limit *limit* [*threshold*]

Parameter	Description
<i>limit</i>	The number of the entries that can be added to the IPv6 multicast routing table is 1 to 2147483647
<i>threshold</i>	(Optional) Number of IPv6 multicast routes at which alarms will be triggered


Defaults

The default value of *limit* is 1024.

The default value of *threshold* is 2147483647.

Command Mode Global configuration mode

This command is used to restrict the number of route adding to the IPv6 multicast table.

 The hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.

Usage Guide

Packets that exceed this value will be discarded.. If you want to use the PIM protocol to create more than 128 entries in the multicast routing table, you are advised to set the CPP value of PIM packets to the number of entries in the multicast routing table. If you want to use the IGMP protocol to create more than 1000 entries in the multicast routing table, you are advised to set the CPP value of IGMP packets to the number of entries in the multicast routing table.

Configuration The following example sets the route limit to 500 and the warning value 90.

Examples

```
Ruijie(config)# ipv6 multicast route-limit 500 90
```

2.6 ipv6 multicast rpf longest-match

Use the RPF rule to select the static multicast route, MBGP route and the unicast route for the purpose of RPF check from the static multicast route list, the MBGP route list and the unicast route list.

Use this command to select one route with the longest-matched mask from the above-mentioned three routes. If the priority values of all three routes are the same, the routes will be selected in order of static multicast route, MBGP route and unicast route.

Use the **no** form of this command to restore the default setting.

ipv6 multicast rpf longest-match

no ipv6 multicast rpf longest-match

Parameter	Parameter	Description
Description	N/A	N/A

Use the RPF rule to select the static multicast route, MBGP route and the unicast route for the purpose of RPF check from the static multicast route list, the MBGP route list and the unicast route list.

Defaults

Use this command to select one route, which is prior to the other two routes, with the longest-matched mask from the above-mentioned three routes. If the priority values of all three routes are the same, the routes will be selected in order of static multicast route, MBGP route and unicast route.

Command

Mode Global configuration mode

Usage

Guide N/A

Configuration Examples The following example selects one route with the longest-matched mask from the above-mentioned three routes.

```
Ruijie(config)# ipv6 multicast rpf longest-match
```

2.7 ipv6 multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. Use the **no** form of this command to restore the default setting.

ipv6 multicast static *source-address group-address interface-type interface-number*

no ipv6 multicast static *source-address group-address interface-type interface-number*

Parameter	Description
<i>source-address</i>	Source IPv6 address
<i>group-address</i>	IPv6 address of the multicast group
<i>interface-type interface number</i>	2-layer interface on which multicast packets are allowed to forward

Defaults This function is disabled by default.

Command

Mode Global configuration mode

You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces.

Usage Guide This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-SMv6) may be affected because some features of the multicast protocol are driven by multicast flows.

Configuration Examples The following example configures forwarding multicast flows (2222::3333, ff66::100) through GigabitEthernet 2/6 and FastEthernet 3/2.

```
Ruijie(config)# ipv6 multicast static 2222::3333 ff66::100 G2/6
```

```
Ruijie(config)# ipv6 multicast static 2222::3333 ff66::100 F3/2
```

2.8 ipv6 multicast-routing

Use this command to enable the IPv6 multicast routing forwarding. Use the **no** form of this command to restore the default setting.

ipv6 multicast-routing

no ipv6 multicast-routing


Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default

Command Mode Global configuration mode

Use this command to enable the IPv6 multicast routing forwarding. With this function disabled, the multicast protocol cannot be enabled.

Usage Guide

 This command must be configured to enable the IPv6 multicast routing forwarding. This function conflicts with IGMP Snooping.

Configuration The following example enables the IPv6 multicast routing forwarding.

Examples Ruijie(config)# ipv6 multicast-routing

2.9 msf6 nsf

Use this command to configure parameters for multicast non-stop forwarding. Use the no form of this command to restore the default setting.

msf6 nsf { convergence-time *time* | leak *interval* }

no msf6 nsf { convergence-time | leak }

Parameter	Parameter	Description
Description	convergence-time <i>time</i>	Maximum duration for which the system waits for multicast protocol convergence The unit is second. The value ranges from 0 to 3600.
	leak <i>interval</i>	Interval at which multicast packets are leaked The unit is second. The value ranges from 0 to 3600.

Defaults The default convergence-time is 20 seconds and leak interval is 30 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum duration for which the system waits for multicast protocol convergence.

```
Ruijie (config)# msf6 nsf convergence-time 300
```

The following example sets the interval at which multicast packets are leaked.

```
Ruijie (config)# msf6 nsf leak 200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.10 show ipv6 mrf6 mfc

Use this command to display the IPv6 multicast forwarding table.

show ipv6 mrf6 mfc [*v6source-address v6group-address*]

Parameter	Parameter	Description
Description	<i>v6group-address</i>	IPv6 address of a multicast group
	<i>v6source-address</i>	IPv6 address of a multicast source

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display the entries of the multicast data stream forwarding table. The forwarding table displayed in the command output is basically consistent with the multicast routing forwarding table displayed in the command output of **show ipv6 mroute**. The difference is that in the multicast data stream forwarding table, the protocols based on which entries are generated are not recorded.

The two parameters are optional. The source address and group address must be specified together. If the two parameters are not specified, all mrf table entries will be displayed.

If the two parameters are specified, the mrf entries of the specified source address and group address are displayed.

Configuration Examples The following example displays the 3-layer multicast forwarding table entries of IPv6 (the source address is 2000::1 and the group address is FF55::1).

```
Ruijie#show ipv6 mrf6 mfc 2000::1 FF55::1
Multicast Routing and Forwarding Cache6 Table
(2000::1, FF55::1)
FAST_SW, SWTCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0
Incoming interface: VLAN 1[4097]
Outgoing interface list:
VLAN 3 (1)
```

Field	Description
2000::1	Source address of entries
FF55::1	Group address of entries
FAST_SW	Indicates whether the entries allow fast forwarding, that is, whether the entries can be forwarded by using hardware or software forwarding. If the entries include an interface that does not support the multicast function (for example, the GRE tunnel interface), fast forwarding is not allowed.
SWTCHED	Indicates whether the entries have been placed in the forwarding table on the next layer.
MIN_MTU MTU	Minimum MTU value of entries
MIN_MTU_IFINDEX	Index of the interface that has the minimum MTU value
WRONG IF	Number of multicast packets sent from the wrong inbound interface
VLAN 1[4097]	Indicates that the rpf inbound interface is VLAN1. 4097 indicates the IFINDEX of the interface.
VLAN 3 (1)	Indicates that the 3-layer outbound interface of the entries is VLAN 3. 1 indicates the ttl threshold of the 3-layer interface.

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

2.11 show ipv6 mroute

Use this command to display the IPv6 multicast forwarding table.

show ipv6 mroute [*group-or-source-address* [*group-or-source-address*]] [**sparse**] [**summary** | **count**]

Parameter Description

Parameter	Description
<i>v6group-address</i>	Multicat group IPv6 address
<i>v6source-address</i>	Multicast source IPv6 address
sparse	Displays the core entry of the multicast routing table.
summary	Displays the summary of the multicast routing table.
count	Displays the count of the multicast routing table.

Command**Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

The following example displays all information of the IPv6 multicast routing table.

```
Ruijie# show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SMv6, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example displays the count of the routing table.

```
Ruijie# show ipv6 mroute count
IPv6 Multicast Statistics
Total 1 routes using 168 bytes memory
Route limit/Route threshold: 1024/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 77/147/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 77/147/0
Immediate/Timed stat updates sent to clients: 0/29
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:09
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(2222::1234, ff56::1234), Forwarding: 1/0, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example displays the summary of the routing table.

```
Ruijie# show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), 00:00:28/00:03:25, PIM-SMv6, Flags: TF
```

**Configuratio
n Examples****Related
Commands**

Command	Description
clear ipv6 mroute	N/A

clear ipv6 mroute statistics	N/A
-------------------------------------	-----

2.12 show ipv6 mroute static

Use this command to display the static IPv6 multicast routing information.

show ipv6 mroute static

Parameter	Parameter	Description
Description	N/A	N/A

Command

Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage This command is used to display the statically-configured multicast route. Under the same condition,
Guide the static multicast route is prior to the unicast route.

The following example displays the static IPv6 multicast routing information.

Configuration	Ruijie#show ipv6 mroute static
Examples	Mroute: 2233::/64, RPF neighbor: 3333::3333 Protocol: , distance: 0

2.13 show ipv6 mvif

Use this command to display the basic information of the multicast interface.

show ipv6 mvif { interface-type interface-number }

Parameter	Parameter	Description
Description	<i>interface-type interface-number</i>	Interface type and number

Command

Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

The following example displays the basic information of the multicast interface of svil.

Configuration	Ruijie#show ipv6 mvif
Examples	<pre> Interface Mif Owner Uptime Idx Module Register 0 03d03h09m VLAN 1 1 PIMSMV6 03d03h09m </pre>

2.14 show ipv6 rpf

Use this command to display the RPF information of the specified source IPv6 address.

show ipv6 rpf *v6source-address*

Parameter	Parameter	Description
Description	<i>v6source-address</i>	Specified source IPv6 address

Command

Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

The following example displays the information of the RPF to 2222::3333:

```
Ruijie# show ipv6 rpf 2222::3333
RPF interface: GigabitEthernet 0/1
RPF neighbor: ::
RPF route: 2222::/64
RPF type: unicast (connected)
RPF recursion count: 0
Doing distance-preferred lookups across tables
Distance: 0
Metric: 0
```

Configuration

Examples

2.15 show msf6 msc

Use this command to display entries of the IPv6 routing multicast data stream exchange table.

show msf6 msc [*v6source-address*] [*v6group-address*] [*vlan-id*]

Parameter	Parameter	Description
Description	<i>v6group-address</i>	IPv6 address of a multicast group
	<i>v6source-address</i>	IPv6 address of a multicast source
	<i>vlan-id</i>	VLAN ID of the inbound interface of the entries If the value is greater than 4096, the interface is a routing interface.

Defaults N/A

Command Privileged EXEC mode/Global configuration mode/Interface configuration mode

Mode

Usage Guide This command is used to display entries of the IPv6 routing multicast data stream exchange table.

The three parameters are all optional.

If only the source address is specified and set to s1, msc entries of this source address will be

displayed.

If the source address is set to s1 and the group address is set to g1, msc entries of this source address and group address will be displayed.

If the source address is set to s1, the group address is set to g1, and the VLAN ID is set to v1, then msc entries that meet these three conditions will be displayed.

You must specify these three parameters in sequence. That is, you must specify the current parameter before specifying the next.

Configuration Examples The following example displays entries of the IPv6 routing multicast data exchange table of source address 2000::1:

```
Ruijie# show msf6 msc 2000::1
Multicast Switching Cache Table
(2000::1, FF55::1, 1), SYNC, MTU:0, 1 OIFs
  VLAN 4094(8190): 1 OPORTs, REQ: DONE
  OPORT 6, MLD-SNP, REQ: DONE
```

Field	Description
2000::1	Source address of entries
FF55::1	Group address of entries
1	VLAN ID of the inbound interface of the entries
SYNC	Indicates that the entries have been synchronized to the bottom-layer hardware.
MTU	MTU value of the entries
OIFs	Number of 3-layer interfaces of the entries
VLAN 4094(8190)	Indicates a 3-layer outbound interface VLAN xxx (yyy). If the 3-layer interface is an SVI interface, the value of xxx is the VLAN VID of the SVI, and the value of yyy is the VLAN vid+4096. If the 3-layer interface is a routing interface, the value of xxx is the IFINDEX of the interface+4096, and the value of yyy is the IFINDEX. This facilitates the index management of all 3-layer interfaces.
1 OPORTs	Number of 2-layer interfaces owned by this 3-layer exit oif
REQ: DONE	Indicates that the oif has been set to the bottom-layer hardware. The value may be: Waiting to be added. Usually it is waiting for a data stream to be triggered. DEL: Being deleted. DONE: Synchronized to the hardware.
OPORT 6	Indicates that the oif has a 2-layer interface with the interface number of 6.
MLD-SNP	Indicates that the interface is created based on MLD SNOOPING. Alternatively, the value may be one of the following options: ROUTER: Indicates that the interface is created based on the 3-layer protocol. INHERIT_FM_MLD_SNP: Indicates that the interface is created based on the MLD SNOOPING protocol inherited from other entries.
REQ: DONE	Indicates that the interface has been set to the bottom-layer hardware. The value may be: ADD: Waiting to be added. Usually it is waiting for a data stream to be triggered. DEL: Being deleted. DONE: Synchronized to the hardware.

Related	Command	Description
Commands	N/A	N/A

Platform N/A
Description

2.16 show msf6 nsf

Use this command to display the multicast non-stop forwarding configuration.

show msf6 nsf

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the multicast non-stop forwarding configuration.

Examples

```
Ruijie# show msf6 nsf
Multicast HA Parameters
-----+-----+
protocol convergence timeout      120 secs
flow leak interval                 20 secs
```

Related	Command	Description
Commands	msf6 nsf	Multicast non-stop forwarding

Platform N/A
Description

3 IGMP Commands

3.1 clear ip igmp group

Use this command to clear dynamic group member information obtained from the response messages in the IGMP buffer.

```
clear ip igmp group [ group-address [ interface-type interface-number ] ]
```

Parameter Description	Parameter	Description
	<i>group-address</i>	32-bit multicast group IP address
	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The IGMP buffer includes a list that contains the multicast groups that the hosts in the direct subnet join. If the device joins a group, this group will be included in this list. To delete all the entries from the IGMP buffer, use the **clear ip igmp group** command without parameters.

Configuration The following example clears all group entries.

Examples

```
Ruijie# clear ip igmp group
```

Related Commands	Command	Description
	show ip igmp groups	N/A
	show ip igmp interface	N/A

Platform Description N/A

3.2 clear ip igmp interface

Use this command to clear the IGMP entry for the interface.

```
clear ip igmp interface interface-type interface-number
```

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>interface-type</i>	Interface type
<i>interface-number</i>	Interface number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the information on the interface that is generated when IGMP is configured. The information includes the number of report/leave packets, and group members on interfaces.

Configuration The following example clears the IGMP entry for the interface.

Examples Ruijie# clear ip igmp interface gi 0/1

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.3 ip igmp access-group

Use this command to control a multicast group on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp access-group *access-list*

no ip igmp access-group


default ip igmp access-group

Parameter Description	Parameter	Description
	<i>access-list</i>	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.

Defaults This command is disabled by default.

Command Mode Interface configuration mode

Usage Guide You can add several multicast groups into the specific interfaces of the host in a subnet. These multicast groups can be controlled using **ip igmp access-group**.

 With the IGMPv3 enabled, when the multicast group accesses the control command, the extended ACL is associated. If the IGMP report information received is (S1, S2, S3...Sn, G), the corresponding ACL will be used by this command to the (0, G) for the matching check. In order to use this command normally, the (0, G) must be configured explicitly for the extended ACL so as to implement the normal filtering of (S1, S2, S3...Sn, G).

Configuration The following example adds the interface Ethernet 0/1 to the group 225.2.2.2.

Examples

```
Ruijie# configure terminal
Ruijie(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Ruijie(config)# interface ethernet 0/1
```

The following example associates the group control list with the extended ACL on the interface Eth 0/1 which only processes the igmp protocol packets with source address 1.1.1.1 and group address 233.3.3.3.

```
Ruijie# configure terminal
Ruijie(config)# ip access-list extended ext_acl
Ruijie(config-ext-nacl)# permit ip host 1.1.1.1 host 233.3.3.3
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp access-group ext_acl
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

3.4 ip igmp enforce-router-alert

Use this command to receive IGMP packets with **router-alert** option , and discard those without the option.

ip igmp enforce-router-alert

Use the **no** form of this command to receive all IGMP packets.

no ip igmp enforce-router-alert

Use the **default** form of this command to restore the default setting.

default ip igmp enforce-router-alert

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage N/A

Guide

Configuration Examples The following example receives IGMP packets with **router-alert** option.

```
Ruijie# configure terminal
Ruijie(config)# ip igmp enforce-router-alert
```

Platform N/A

Description

3.5 ip igmp enforce-source-subnet

Use this command to receive only the IGMP report packet containing the source address in the same network segment as the port.

ip igmp enforce-source-subnet

Use the no form of this command to restore the default setting.

no ip igmp enforce-source-subnet

Use the default form of this command to restore the default setting.

default ip igmp enforce-source-subnet

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The source IP address is not checked by default.

Command Global configuration mode

Mode

Usage N/A

Guide

Configuration Examples The following example receives only the IGMP report packet containing the source address in the same network segment as the port.

```
Ruijie# configure terminal
Ruijie(config)# ip igmp enforce-source-subnet
```

Platform N/A

Description

3.6 ip igmp immediate-leave group-list

In the IGMPversion2 and IGMPversion3 versions, use this command to shorten the delay of leaving a group. This command is used when a single receiving host is connected to a single interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp immediate-leave group-list *access-list*

no ip igmp immediate-leave

default ip igmp immediate-leave

Parameter Description	Parameter	Description
	<i>access-list</i>	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.

Defaults This function is disabled by default.

Command

Mode Interface configuration mode

Usage Guide If this command is not configured, the device will send a particular group query message upon receiving the leaving message from the interface. When the host response is timeout, the device stops forwarding packets to this interface. The length of timeout depends on the query interval of the last member and IGMP robustness variable. The default value is 2s.

If this command is configured, the device does not send a particular group query message upon receiving the leaving message from the interface. Instead, it directly removes this interface from the IGMP buffer and notifies the IGMP protocol. This will shorten the time significantly.

Configuration Examples The following example provides the immediate leaving function for some multicast groups. Certainly, you must make sure each interface of these multicast groups have one group member only.

```
Ruijie# configure terminal
Ruijie(config)# access-list 1 permit 225.192.20.0 0.0.0.255
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp immediate-leave group-list 1
Ruijie(config-if-Ethernet 0/1)# exit
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.7 ip igmp join-group

Use this command to configure the interface of the switch with host activities and adds it to a multicast group, so that the sub-switch can learn the corresponding group information. You can use this command to add an interface to a group.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp join-group *group-address*

no ip igmp join-group *group-address*

default ip igmp join-group *group-address*

Parameter	Parameter	Description
Description	<i>group-address</i>	Multicast group IP address

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command enables the host activities for the IGMP interface. When the host function is enabled, the interface can initiate the report message and respond to the query message. If the IGMP function is enabled on the interface, the interface can initiate the report message, so that the interface can learn the configured group members. You can use this command to add an interface to a group.

Configuration The following example adds a host group member manually.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fast 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp join-group 233.3.3.3
Ruijie(config-if-Ethernet 0/1)# exit
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.8 ip igmp last-member-query-count

Use this command to configure the value of **last-member-query-count**.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp last-member-query-count *number*

no ip igmp last-member-query-count

default ip igmp last-member-query-count

Parameter Description	Parameter	Description
	<i>number</i>	Value of the last member query count in the range from 2 to 7.

Defaults The default is 2.

Command Mode Interface configuration mode

Usage Guide This command only supports IGMPv2 and IGMPv3.
 When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **last-member-query-count** time. The device will delete information about this group member if no group member report is received within the waiting time.
 The waiting time = last-member-query-interval * last-member-query-count + 1/2 * query-max-response-time

Configuration Examples The following example sets the value of last member query count to 3.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0
Ruijie(config-if-Ethernet 0/1)# ip igmp last-member-query-count 3
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.9 ip igmp last-member-query-interval

Use this command to set the time interval of sending the group query message.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval

default ip igmp last-member-query-interval

Parameter Description	Parameter	Description
	<i>interval</i>	The interval sending the group query message in the range from 1 to

	255 in the unit of 0.1 second.
--	--------------------------------

Defaults The default is 10 (1 second).

Command Mode Interface configuration mode

Usage Guide This command only supports IGMPv2 and IGMPv3.
 When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying **last-member-query-count** time. The device will delete information about this group member if no group member report is received within the waiting time.
 The waiting time = last-member-query-interval * last-member-query-count + 1/2 * query-max-response-time

Configuration Examples The following example sets the interval of sending the group query message to 20 seconds.

```
Ruijie# configure terminal
Ruijie(config)# interface eth 0
Ruijie(config-if-Ethernet 0/1)# ip igmp last-member-query-interval 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 ip igmp limit

Use this command to globally set the maximum number of IGMP group records.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit

default ip igmp limit

Parameter Description

Parameter	Description
<i>number</i>	Maximum number of IGMP states, depending on devices
except <i>access-list</i>	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.

Defaults Global: 65,536
 Interface:1,0124

Command Global configuration mode/Interface configuration mode

Mode

Usage Guide Use this command to configure the maximum number of IGMP group records globally or on interfaces. The messages of the members exceeding the threshold will not be saved in the IGMP buffer and will not be forwarded. The messages of the members will be ignored if they exceed the interface or global configuration. If the configured value in global configuration mode is less than that in interface configuration mode, take the former.

Configuration Examples The following example sets the maximum number to 400 globally and to 300 on interfaces except ACL 1.

```
Ruijie# configure terminal
Ruijie(config)# ip igmp limit 400 except acl1
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp limit 300 except acl1
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

3.11 ip igmp mroute-proxy

Use this command to configure an interface as an mroute-proxy interface that can transmit messages to its uplink ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp mroute-proxy *interface-type interface-number*

no ip igmp mroute-proxy

default ip igmp mroute-proxy

Parameter Description

Parameter	Description
<i>interface-type</i>	Name of the relevant uplink interface
<i>interface-number</i>	

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide Use the **ip igmp proxy-service** command to set the uplink interface as the **proxy-service** interface. Use the **ip igmp mroute-proxy** command to set the downlink interface as the **mroute-proxy**

interface.

IGMP query packets are forwarded from the **proxy-service** interface to the **mroute-proxy** interface.

IGMP report packets are forward reversely.

Configuration The following example configures E0/1 as **proxy-service** E0/2 as **mroute-proxy**.

Examples

```
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp proxy-service
Ruijie(config-if-Ethernet 0/1)# exit
Ruijie(config)# interface eth 0/2
Ruijie(config-if-Ethernet 0/2)# ip igmp mroute-proxy
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

3.12 ip igmp proxy-service

Use this command to enable the service function of all downlink **mroute-proxy** ports.

If you run this command on an interface, the interface becomes the uplink port of the corresponding **mroute-proxy** that associates its downlink ports and maintains the group information reported by the downlink ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp proxy-service

no ip igmp proxy-service

default ip igmp proxy-service

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

N/A

**Command
Mode**

Interface configuration mode

Usage Guide

Use the **ip igmp proxy-service** command to set the uplink interface as the **proxy-service** interface.

Use the **ip igmp mroute-proxy** command to set the downlink interface as the **mroute-proxy** interface.

The command can configure at most 32 proxy-service ports. The number of interface with IGMP Proxy enabled is limited by the supported multicast interface number. When receiving a query

message, the **proxy-service** port responds according to the IGMP group member information maintained by the port itself. The member information maintained by the **proxy-service** port is collected from the interface configured with **mroute-proxy**. Therefore, if a port is configured with proxy-service, the port performs the host activities, but not the device activities.

If **switch port** operation is performed on an interface with proxy-service command configured, the **ip igmp mroute-proxy interface** command configured on the associated downlink ports is automatically deleted.

Configuration The following example configures E0/1 as **proxy-service** and E0/2 as **mroute-proxy**.

Examples

```
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp proxy-service
Ruijie(config-if-Ethernet 0/1)# exit
Ruijie(config)# interface eth 0/2
Ruijie(config-if-Ethernet 0/2)# ip igmp mroute-proxy
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

3.13 ip igmp query-interval

Use this command to configure the query interval of an ordinary member.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp query-interval *seconds*

no ip igmp query-interval

default ip igmp query-interval

Parameter Description

Parameter	Description
<i>seconds</i>	Query interval of ordinary member, in the range is from 1 to 18,000 in the unit of seconds.

Defaults

The default is 125 seconds.

Command Mode

Interface configuration mode

Usage Guide

The time to query an ordinary member can be changed by configuring the query interval of the ordinary member.

Configuration

The following example configures the query interval of ordinary member to 120 seconds on the

Examples

interface Ethernet 0.

```
Ruijie(config-if)# ip igmp query-interval 120
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

3.14 ip igmp query-max-response-time

Use this command to configure the maximum response interval.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

default ip igmp query-max-response-time

**Parameter
Description**

Parameter	Description
<i>seconds</i>	The maximum response interval, in the range from 1 to 25 seconds

Defaults

The default is 10 seconds.

**Command
Mode**

Interface configuration mode

Usage Guide

This command controls the interval for the respondent to respond the query message before the device deletes the group information.

**Configuration
Examples**

The following example configures the maximum response interval to 20 seconds on the interface Ethernet 0.

```
Ruijie(config-if-Ethernet 0/1)# ip igmp query-max-response-time 20
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

3.15 ip igmp query-timeout

Use this command to configure the time the device waits before it takes over as the querier.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp query-timeout *seconds*

no ip igmp query-timeout

default ip igmp query-timeout

Parameter Description	Parameter	Description
	<i>seconds</i>	Time the device waits before it takes over as the querier, in the range from 60 to 300 in the unit of seconds.

Defaults The default is 255 seconds.

Command Mode Interface configuration mode

Usage Guide This device becomes the querier if no query packet is received in this duration.

Configuration Examples The following example configures the time the device waits before it takes over as the querier to 200 s seconds on the interface Ethernet 0/1.

```
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp query-timeout 200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.16 ip igmp robustness-variable

Use this command to change the value of the robustness variable.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp robustness-variable *number*

no ip igmp robustness-variable

default ip igmp robustness-variable

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>number</i>	The value of robustness variable, in the range from 2 to 7
---------------	--

Defaults The default is 2.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the value of robustness variable to 3.

```
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp robustness-variable 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.17 ip igmp send-router-alert

Use this command to send IGMP report packets with the Router Alert option.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp send-router-alert

no ip igmp send-router-alert

default ip igmp send-router-alert

Parameter Description

Parameter	Description
N/A	N/A

Defaults The Router Alert option is not carried in IGMP packets by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sends IGMP report packets with the Router Alert option.

```
Ruijie# configure terminal
Ruijie(config)# ip igmp send-router-alert
```

Platform N/A

Description

3.18 ip igmp ssm-map enable

Use this command to enable the **igmp ssm-map** function in the global configuration mode.

Use the **no** form of this command to restore the default setting.

ip igmp ssm-map enable

no ip igmp ssm-map enable

default ip igmp ssm-map enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide If this command is configured, the dynamically learned group information is added forcibly to the associated source record. This command is usually used together with the **ip igmp ssm-map static** command.

Configuration Examples The following example enables the **igmp ssm-map** function in the global configuration mode.

```
Ruijie(config)# ip igmp ssm-map enable
```

```
Ruijie(config)# ip igmp ssm-map static 11 192.168.2.2.
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.19 ip igmp ssm-map static

Use this command to map the static **ssm-map** source IP address to the group records.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp ssm-map static access-list source-address

no ip igmp ssm-map static access-list source-address

default ip igmp ssm-map enable access-list source-address

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
<i>access-list</i>	ACL name in the range 1 to 99, 1,300 to 1,999 or characters.
<i>source-address</i>	Unicast address mapped to the group record.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used together with the **ip igmp ssm-map enable** and **ip igmp ssm-map static** command. After configuration, the port maps the corresponding source IP address to all received messages below **v3**.

Configuration Examples The following example maps the source address 192.168.2.2 to all group records permitted by ACL 11.

```
Ruijie(config)# ip igmp ssm-map enable
Ruijie(config)# ip igmp ssm-map static 11 192.168.2.2.
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.20 ip igmp static-group

Use this command to directly add an interface to a group.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp static-group *group-address*

no ip igmp static-group *group-address*

default ip igmp static-group *group-address*

Parameter Description	Parameter	Description
	group-address	

Defaults The switch is not added to a multicast group by default.

Command Mode Interface configuration mode

Usage Guide This command directly adds an interface to a multicast group. The difference from **join-group** is that it directly adds an interface to the group without interacting with a report message.

You can use this command to add an interface to a group.

The added interfaces by this command can only be deleted by using the **no ip igmp static-group** command.

Configuration The following example adds a host group member.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp static-group 236.6.6.6
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

3.21 ip igmp version

Use this command to set the version number of IGMP to be used on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp version { 1 | 2 | 3 }

no ip igmp version

default ip igmp version

**Parameter
Description**

Parameter	Description
1	IGMP v1
2	IGMP v2
3	IGMP v3

Defaults The default is IGMPv2.

**Command
Mode** Interface configuration mode

Usage Guide Use this command to globally configure the IGMP version. It should be noted that IGMP will reset after configuration.

Configuration The following example sets the version number to 3.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ip igmp version 3
```

Related

Command	Description
---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

3.22 show ip igmp groups

Use this command to display the groups directly connected to the device and the group information learnt from IGMP.

show ip igmp groups [*interface-type interface-number*] [*group-address*] [**detail**]

Parameter Description	Parameter	Description
	<i>group-address</i>	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface number
	detail	Displays the detailed information

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without any parameters to display group address, interface type, and information about all the multicast groups directly connected to the interface. Information about a specific group is displayed if a group address is added to the command.

Configuration Examples The following example displays information about all the groups.

```
Ruijie# show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface  Uptime  Expires  Last Reporter
224.0.1.1     eth2      00:00:09  00:04:17  10.10.0.82
224.0.1.24    eth2      00:00:06  00:04:14  10.10.0.84
224.0.1.40    eth2      00:00:09  00:04:15  10.10.0.91
224.0.1.60    eth2      00:00:05  00:04:15  10.10.0.7
239.255.255.250 eth2      00:00:12  00:04:15  10.10.0.228
239.255.255.254 eth2      00:00:08  00:04:13  10.10.0.84
```

The following example displays detailed information about a specific group.

```
Ruijie# show ip igmp groups 224.1.1.1 detail
Interface      : eth1
Group: 224.1.1.1
Uptime: 00:00:42
```

```

Group mode: Include
Last reporter: 192.168.50.111
TIB-A Count: 2
TIB-B Count: 0
Group source list: (R - Remote, M - SSM Mapping)
Source Address Uptime v3 Exp Fwd Flags
192.168.55.55 00:00:42 00:03:38 Yes R
192.168.55.66 00:00:42 00:03:38 Yes R

```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.23 show ip igmp interface

Use this command to display the information of this interface.

show ip igmp interface [*interface-type interface-number*]

**Parameter
Description**

Parameter	Description
<i>interface-type</i>	Interface type.
<i>interface-number</i>	Interface number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Run this command without any parameter, and all interface information is displayed by default.

Configuration Examples The following example displays the information of all the interfaces.

Examples

```

Ruijie# show ip igmp interface
Interface vlan 1(Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds

```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.24 show ip igmp ssm-mapping

Use this command to display the **ssm-map** information of the IGMP configuration.

show ip igmp ssm-mapping [*group-address*]

Parameter Description	Parameter	Description
	<i>group-address</i>	

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Run this command without any parameter, and all SSM-MAP information is displayed.

Configuration The following example displays the **ssm-map** configuration information.

Examples

```
Ruijie#show ip igmp ssm-mapping 233.3.3.3
Group address: 233.3.3.3
Database      : Static
Source list   : 192.3.3.3
               : 3.3.3.3
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4 MLD Commands

4.1 clear ipv6 mld group

Use this command to clear the dynamic group member learned by MLD protocol.

clear ipv6 mld group [*group-address*] [*interface-type interface-number*]

Parameter Description	Parameter	Description
	<i>group-address</i>	IPv6 multicast group address with 128 bits
	<i>interface-type</i>	The associated interface type
	<i>interface-number</i>	The associated interface number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide MLD maintains a list of the multicast groups to be added to the host in the directly-connected sub-net. Use the **clear ipv6 mld group** command to remove all dynamic group member record from the MLD group member list.

Configuration Examples The following example clears all group records.

```
Ruijie# clear ipv6 mld group
```

The following example clears one group record.

```
Ruijie# clear ipv6 mld group ff1e::100
```

The following example s clears the record on a specified interface.

```
Ruijie# clear ipv6 mld group ff1e::100 interfa fa0/1
```

Related Commands	Command	Description
	show ipv6 mld groups	N/A
	show ipv6 mld interface	N/A

Platform N/A

Description

4.2 clear ipv6 mld interface

Use this command to clear all MLD statistical information and the group member records on the interface.

clear ipv6 mld interface *interface-type interface-number*

Parameter Description	Parameter	Description
	<i>interface-type</i>	The interface type
	<i>interface-number</i>	The interface ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear all group information and some packet statistical information learned by LDP on the interface. Those packet statistical information include the number of the received report packets, the number of the done packets and the the number of the group members on the interface.

Configuration Examples The following example clears all MLD statistical information and the group member records on the interface.

```
Ruijie# clear ipv6 mld interface fa 1/1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.3 ipv6 mld access-group

Use this command to filter the specific requested group on the interface. Only the report packets in accordance with the corresponding ACL are allowed to be processed.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld access-group *access-list*

no ipv6 mld access-group


default ipv6 mld access-group

Parameter Description	Parameter	Description
	<i>access-list</i>	The IPv6 ACL name

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to filter some groups on the interface and associate with the corresponding ACLs. The correspondent ACL deny report packets will be discarded. This command supports the extended ACL and the source record information of the MLDv2 packets can be filtered.

 The multicast group access control command is associated with the extended ACL. When the received MLD report message is (S1,S2,S3...Sn,G), use this command to match and check the (0,G) message using the corresponding ACL. To this end, a (0,G) must be configured for the extended ACL to filter the (S1,S2,S3...Sn,G).

Configuration Examples The following example enables the group information carried in the report packets to be in accordance with acl for the normal handling on the interface Eth0/1.

```
Ruijie(config)#ipv6 access-list acl
Ruijie(config-ipv6-acl)#permit ipv6 ::/64 ff66::100/64
Ruijie(config-ipv6-acl)#permit ipv6 2222::3333/64 ff66::100/64
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld access-group acl
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

4.4 ipv6 mld immediate-leave group-list

Use this command to set the immediate-leave mechanism. With this command configured, the group within the range of group-list, will not send the query packet for the specific group and will remove this group from the group member list immediately after receiving the corresponding done packets. This function is used in the condition that there is only one multicast source that receives the host request on an interface. Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld immediate-leave group-list *access-list*
no ipv6 mld immediate-leave group-list
default ipv6 mld immediate-leave group-list

Parameter Description

Parameter	Description
<i>access-list</i>	The IPv6 ACL name

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Without this command configured, when the device receives the MLD leave packets, the request packets for the specific groups will be sent. If there is still no host reply within the response time, the device will remove the corresponding group record from the group member list. The timeout interval is determined by the last member query interval and the MLD robustness variable, and the default value is 2 seconds.

With this command configured, when the device receives the MLD leave packets, it will not send the request packets for the specific groups, but remove the group information immediately, which reduces the leave delay greatly in the condition that there is only one host connecting to the interface.

Configuration The following example configures the immediate-leave function.

```
Examples Ruijie# configure terminal
Ruijie(config)#ipv6 access-list acl
Ruijie(config-ipv6-acl)#permit ipv6 2222::3333/64 ff66::100/64
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld immediate-leave
group-list acl
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

4.5 ipv6 mld join-group

Use this command to configure the host action for the switch interface and add the related multicast group to the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld join-group *group-address*

no ipv6 mld join-group *group-address*

default ipv6 mld join-group *group-address*

**Parameter
Description**

Parameter	Description
<i>group-address</i>	The IPv6 non-management multicast group address, which cannot start with 0xFF*1, 0xFF*2, and 0xFF3*

Defaults The interface is not added to any group by default.

**Command
Mode** Interface configuration mode

Usage Guide Use this command to enable the MLD host action on the interface. The interface can not only send the packets initiatively, but also reply to the query packets.
Use this command if it is necessary to join a group member to the interface.

Configuration The following example adds the host group member:

Examples

```
=
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld join-group ff55::100
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

4.6 ipv6 mld last-member-query-count

Use this command to set the last-member-query-count number.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld last-member-query-count *number*

no ipv6 mld last-member-query-count

default ipv6 mld last-member-query-count

Parameter Description

Parameter	Description
<i>number</i>	The last member query count number. The valid range is 2 to 7.

Defaults The default is 2.

Command Mode Interface configuration mode

Usage Guide With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group (multiplied by the value of **mld last-member-query-count**) plus half the reply time.

Configuration The following example sets the last-member-query-count number to 3.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld last-member-query-count 3
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.7 ipv6 mld last-member-query-interval

Use this command to set the time interval of sending the query packets to the specific group.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld last-member-query-interval *interval*

no ipv6 mld last-member-query-interval

default ipv6 mld last-member-query-interval

Parameter Description	Parameter	Description
	<i>interval</i>	

Defaults The default is 10 seconds.

Command Mode Interface configuration mode

Usage Guide With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group(multiplied by the value of **mld last-member-query-count**) plus half the reply time.

Configuration Examples The following example sets the mld last-member-query-interval to 2 seconds.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld last-member-query-interval 20
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.8 ipv6 mld limit

Use this command to enable to learn the max-number of the group member through the MLD protocol.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld limit *number* [**except** *access-list*]

no ipv6 mld limit *number* [**except** *access-list*]

default ipv6 mld limit *number* [**except** *access-list*]

Parameter Description	Parameter	Description
	<i>number</i>	The maximum number of the group member learned by the MLD
	except <i>access-list</i>	(Optional) The ACL beyond the configured mld limit

Defaults Interface: 1,024
Global: 65,536

Command Mode Interface configuration mode/Global configuration mode

Usage Guide Use this command to set the max-number of the group members learned through the MLD in the global configuration mode. If the group member number has exceeded the limit, the received report packets later will be discarded and fail to form the group record.
If the except list has also been set at the same time, the group member packets, including the packets in the access-list, will be free from the member number limit.
This command can also be used in the interface configuration mode. The configurations in two different configuration modes are independent. If the number limit in the global configuration mode is lower than the one in the interface configuration mode, the former configuration takes precedence.

Configuration Examples The following example sets the MLD limit to 400, but the configured ACL can still learn.

```
Ruijie(config-if)# ipv6 mld limit 300 except acl
Ruijie# configure terminal
Ruijie(config)# ipv6 mld limit 400 except acl1
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld limit 300 except acl1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.9 ipv6 mld mroute-proxy

Use this command to enable the interface to forward the packets to the correspondent connected interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld mroute-proxy *interface-type interface-number*

no ipv6 mld mroute-proxy

default ipv6 mld mroute-proxy

Parameter	Parameter	Description
Description	<i>interface-type</i> <i>interface-number</i>	The correspondent connected interface

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide Use the **ipv6 mld proxy-service** command to configure the uplink interface as **proxy-service** one. Use the **ipv6 mld mroute-proxy** command to configure the downlink interface as **mroute-proxy** one. After the connected interface has been configured as the proxy-service interface, it can forward the MLD packets sent from other members.

Configuration The following example sets the interface as the mroute-proxy interface and enables multicast proxy.

Examples

```
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld proxy-service
Ruijie(config-if-Ethernet 0/1)# exit
Ruijie(config)# interface eth 0/2
Ruijie(config-if-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.10 ipv6 mld proxy-service

Use this command to enable the proxy-service function for the interface connected with the mroute-proxy interface in the downward direction. After configuring this command, the interface becomes the one connected with the mroute-proxy in the upward direction, and associates with and

maintains the group information from the interfaces in the downward direction. Use the **no** or **default** form of this command to disable the default setting.

ipv6 mld proxy-service

no ipv6 mld proxy-service

default ipv6 mld proxy-service

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide Use the **ipv6 mld proxy-service** command to configure the uplink interface as **proxy-service** one. Use the **ipv6 mld mroute-proxy** command to configure the downlink interface as **mroute-proxy** one. The configurable max-number limit is 32. The number of the interfaces with MLD Proxy enabled is limited by the number multicast interfaces supported device. After receiving the query packet, the proxy-service interface replies according to the member information, which are collected from the mroute-proxy interface and maintained by the proxy-service interface itself. With proxy-service configured, this interface owns the host action rather than the router action. The **ipv6 mld mroute-proxy interface** command configuration on the associated interface in the downward direction is removed automatically if the switchport operation is performed on the interfaces.

Configuration The following example sets the interface proxy-service and enables multicast proxy.

Examples

```
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld proxy-service
Ruijie(config-if-Ethernet 0/1)# exit
Ruijie(config)# interface eth 0/2
Ruijie(config-if-Ethernet 0/1-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.11 ipv6 mld querier-timeout

Use this command to set the querier alive period.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld querier-timeout *seconds*
no ipv6 mld querier-timeout
default ipv6 mld querier-timeout

Parameter Description	Parameter	Description
	<i>seconds</i>	The querier alive period, in the range from 60 to 300 in the unit of seconds.

Defaults The default is 255 seconds.

Command Mode Interface configuration mode

Usage Guide After the querier sends the query packet, the querier will wait to receive the query packet sent by another querier within the alive period. If no packet is received by the first querier within the alive period, then the first querier takes itself as the only querier on the network segment.

Configuration Examples The following example sets the querier alive period to 200 seconds.

```
Ruijie(config-if-Ethernet 0/1)# ipv6 mld querier-timeout 200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.12 ipv6 mld query-interval

Use this command to set the query interval for the general member.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld query-interval *seconds*
no ipv6 mld query-interval
default ipv6 mld query-interval

Parameter Description	Parameter	Description
	<i>seconds</i>	The query interval for the general member, in the range from 1 to 18,000 in the unit of seconds.

Defaults The default is 125 seconds.

Command Interface configuration mode

Mode

Usage Guide The interval of the timer for sending the general query packets can be changed by configuring the query-interval for the general member.

Configuration The following example sets the query-interval for the general member on the interface Ethernet 0/1.

Examples Ruijie(config-if-Ethernet 0/1)# ipv6 mld query-interval 120

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.13 ipv6 mld query-max-response-time

Use this command to set the maximum response time.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

default ipv6 mld query-max-response-time

Parameter Description	Parameter	Description
	<i>seconds</i>	

Defaults The default is 10 seconds.

Command Interface configuration mode

Mode

Usage Guide Use this command to control the maximum response time of the host after the device sends the query packets. If there is no response within the maximum response time, MLD will remove the corresponding group from the group member list.

Configuration The following example sets the maximum query response time on the interface Ethernet 0/1.

Examples Ruijie(config-if-Ethernet 0/1)# ipv6 mld query-max-response-time 20

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.14 ipv6 mld robustness-variable

Use this command to set querier robustness value.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld robustness-variable *number*

no ipv6 mld robustness-variable

default ipv6 mld robustness-variable

Parameter Description	Parameter	Description
	<i>number</i>	Sets the querier robustness value, in the range from 2 to 7.

Defaults The default is 2.

Command Interface configuration mode

Mode

Usage Guide N/A

Configuration The following example sets the querier robustness value to 3.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld robustness-variable 3
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.15 ipv6 mld ssm-map enable

Use this command to enable the mld ssm-map function.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld ssm-map enable

no ipv6 mld ssm-map enable

default ipv6 mld ssm-map enable

Parameter Description	Parameter	Description
		N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide With this command configured, the group information dynamically learned will be added to the related source record forcibly. Usually, this command is set with the **ipv6 mld ssm-map static** command.

Configuration Examples The following example enables the mld ssm-map function in the global configuration mode.

```
Ruijie(config)# ipv6 mld ssm-map enable
Ruijie(config)# ipv6 mld ssm-map static 11 4444::1234
```

Related Commands	Command	Description
		N/A

Platform Description N/A

4.16 ipv6 mld ssm-map static

Use this command to set the mld ssm-map static mapping source record in the global configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld ssm-map static *access-list source-address*

no ipv6 mld ssm-map static *access-list source-address*

default ipv6 mld ssm-map static *access-list source-address*

Parameter Description	Parameter	Description
	<i>access-list</i>	Sets the IPv6 ACL name.
	<i>source-address</i>	Sets the unicast address for the group record mapping.

Defaults There is no mapping source address by default.

Command Mode Global configuration mode

Usage Guide This command is used with the **ipv6 mld ssm-map enable** command. With this command configured, the received mldv1 packets are mapped to the correspondent source record.

Configuration The following example maps all group record of the ACL name to the source address 4444::1234.

Examples

```
Ruijie(config)# ipv6 mld ssm-map enable
Ruijie(config)# ipv6 mld ssm-map static te 4444::1234
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.17 ipv6 mld static-group

Use this command to add an interface to a group statically.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld static-group *group-address*

no ipv6 mld static-group *group-address*

default ipv6 mld static-group *group-address*

Parameter Description	Parameter	Description
	<i>group-address</i>	

Defaults The interface is not added to any group statically.

Command Mode Interface configuration mode

Usage Guide Use this command to add a multicast group to the interface directly. The difference from the join-group is that the packet interaction is not necessary. Use this command when it is necessary to add a group member to the interface. It is worth mentioning that only the **no ipv6 mld static-group** command can be used to delete the group, but not the **clear** command.

Configuration The following example adds interface Eth0/1 to group ff55::3 statically.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld static-group ff55::3
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.18 ipv6 mld version

Use this command to set the MLD version number on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld version { 1 | 2 }

no ipv6 mld version

default ipv6 mld version

Parameter Description	Parameter	Description
	{ 1 2 }	Sets the MLD version number.

Defaults The default is 2.

Command Interface configuration mode

Mode

Usage Guide Use this command to control the MLD version number.

Configuration The following example sets the MLD version 1.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld version 1
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.19 show ipv6 mld groups

Use this command to display the group connected with the switch and the group information learned from the MLD.

show ipv6 mld groups [*group-address* | *interface-type interface-number*] [**detail**]

Parameter Description	Parameter	Description
	<i>group-address</i>	Sets the IPv6 multicast group address in 128 bits.

<i>interface-type</i>	Sets the interface type.
<i>interface-number</i>	Sets the interface number.
detail	Displays the information in detail.
	Displays all the group information.

Defaults N/A

Command Mode Privileged EXEC mode/Interface configuration mode

Usage Guide Use this command without the parameters to display the information including the group address, the interface type and the multicast group information. Use this command with a parameter to display the information on a specific group.

Configuration The following example displays all group information.

Examples

```
Ruijie# show ipv6 mld groups
MLD Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
ff66::1 VLAN1 00:10:57 00:02:16 fe80::2d0:f8ff:fe22:3378
```

The following example displays the detailed information.

```
Ruijie# show ipv6 mld groups detail
Interface: VLAN 1
Group: ff66::1
Uptime: 00:10:26
Group mode: Exclude (Expires: 00:02:47)
Last reporter: fe80::2d0:f8ff:fe22:3378
Source list is empty
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.20 show ipv6 mld interface

Use this command to display the configurations on the interface.

show ipv6 mld interface [interface-type interface-number]

Parameter Description

Parameter	Description
<i>interface-type</i>	Sets the interface type.

<i>interface-number</i>	Sets the interface number.
-------------------------	----------------------------

Defaults N/A

Command User EXEC mode/Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the state information of all interfaces.

Examples

```
Ruijie# show ipv6 mld interface
Interface VLAN 2 (Index 4098)
  MLD Enabled, Inactive, Version 2 (default)
  MLD interface limit is 1024
  MLD interface has 0 group-record states
  MLD interface has 1 join-group records
  MLD interface has 0 static-group records
  MLD activity: 0 joins, 0 leaves
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 10 (1/10s)
  Last member query count is 2
  Group Membership interval is 260
  Robustness Variable is 2
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

4.21 show ipv6 mld ssm-mapping

Use this command to display the mapping information of the source address for the group record.

show ipv6 mld ssm-mapping [*group-address*]

**Parameter
Description**

Parameter	Description
<i>group-address</i>	Displays the group address.

Defaults N/A

Command User EXEC mode/Privileged EXEC mode
Mode

Usage Guide N/A

Configuration The following example displays the state information of all interfaces.

Examples

```
Ruijie# show ipv6 mld interface
Interface VLAN 2 (Index 4098)
  MLD Enabled, Inactive, Version 2 (default)
  MLD interface limit is 1024
  MLD interface has 0 group-record states
  MLD interface has 1 join-group records
  MLD interface has 0 static-group records
  MLD activity: 0 joins, 0 leaves
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 10 (1/10s)
  Last member query count is 2
  Group Membership interval is 260
  Robustness Variable is 2
```

**Related
Commands**

Command	Description
N/A	N/A

5 PIM-DM Commands

5.1 clear ip pim dense-mode track

Use this command to clear the statistics of PIM-DM packets.

clear ip pim dense-mode track

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to reconfigure the start time of the statistics and clear the PIM packet counter.

Configuration The following example clears the statistics of PIM-DM packets.

Examples Ruijie# clear ip pim dense-mode track

Related Commands	Command	Description
	show ip pim dense-mode track	Displays the statistics of the PIM packets.

Platform N/A

Description

5.2 ip pim dense-mode

Use this command to enable PIM-DM on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim dense-mode

no ip pim dense-mode








default ip pim dense-mode

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide

-  Before enabling the PIM-DM, enable the multicast forwarding function in the global configuration mode. Otherwise, the multicast data packet cannot be forwarded even the PIM-DM is enabled.
-  Once the PIM-DM is enabled, the IGMP is enabled automatically on the interface without manual configuration.
-  During the execution of this command, if the prompt "Failed to enable PIM-DM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.
-  During the execution of this command, if the prompt "PIM-DM Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured multicast interface number exceeds the upper limit of the multicast interfaces. In this case, if it's still necessary to enable the PIM-DM on the interface, delete the unnecessary PIM-DM, PIM-SM or DVMRP interfaces.
-  It is not recommended to configure different multicast routing protocols on different interfaces of a device.
-  IPv4 multicast function supports only 4Over4, 4Over4 GRE, 4Over6, and 4Over6 GRE on tunnel ports. For those multicast-incapable, through multicast function can be enabled, there are no error prompts and packet multicast transmission.
-  Multicast tunnels can be established only on Ethernet ports, which do not support nested tunneling and multicast QoS/ACL.

Configuration The following example enables PIM-DM on the interface.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim dense-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.3 ip pim dense-mode subvlan

Use this command to enable PIM-DM on a super VLAN. Use the **no** form or **default** form of this command to disable PIM-DM on a super VLAN.

ip pim dense-mode subvlan [all | vid]
no ip pim dense-mode subvlan

default ip pim dense-mode subvlan

Parameter Description	Parameter	Description
	all	Sends packets to all sub VLANs.
	<i>vid</i>	Sends packets to a specified sub VLAN.

Defaults PIM-DM is disabled on super VLANs by default.

Command Mode Interface configuration mode

Usage Guide In most scenarios on the PIM network, the PIM DM protocol does not need to be enabled on interfaces of a super VLAN. In general, a super VLAN includes many sub VLANs. If the PIM DM protocol is enabled on the interfaces of the super VLAN, multicast packets will be replicated and sent to all sub VLANs. As a result, traffic generated easily exceeds the device processing capability, causing protocol flapping. In some scenarios that require the PIM DM protocol to be enabled on the interfaces of the super VLAN, the PIM-DM sub VLAN function may be configured, to send packets to a specified sub VLAN or all sub VLANs.

Configuration Examples The following example enables PIM-DM on VLAN 100 to send packets to its sub VLAN 200.

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 100
Ruijie(config-if-vlan 100)# ip pim dense-mode subvlan 200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.4 ip pim mib dense-mode

Use this command to switch the device from the PIM MIB sparse mode to the PIM MIB dense mode. Use the **no** form or **default** form of this command to switch back to the PIM MIB sparse mode.

ip pim mib dense-mode
no ip pim mib dense-mode
default ip pim mib dense-mode

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults The device is in the PIM MIB sparse mode by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example switches the device from the PIM MIB sparse mode to the PIM MIB dense mode.

```
Ruijie# configure terminal
Ruijie(config)# ip pim mib dense-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.5 ip pim neighbor-filter

Use this command to enable the neighbor filtering on the interface. Use the **no** or **default** form of this command is to restore the default setting.

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter *access-list*

default ip pim neighbor-filter *access-list*

Parameter Description

Parameter	Description
<i>access-list</i>	Access control list supporting numerical ACL in the range from 1 to 99 and name ACL

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide If the neighbor filtering is set, PIM-DM will not establish the peering relationship with this neighbor or will terminate the established peering relationship with this neighbor once the neighbor is denied by the filtering access list.

Configuration The following example enables the neighbor filtering on the interface.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim neighbor-filter 14
```

- i When the associated ACL rule is permit, only the neighbor address in ACL can be used as the PIM neighbor of the current interface. When the associated ACL rule is deny, the neighbor address in ACL cannot be used as the PIM neighbor of the current interface.
- i Peering relationship refers to the interaction of protocol packets between the PIM neighbors. If the peering relationship with a PIM device is terminated, the neighbor relationship with this device will not be established, and the PIM protocol packets from this device will not be received.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.6 ip pim override-interval

Use this command to reconfigure the override-interval of the hello message.

Use the **no** or **default** form of this command to restore the default setting.

ip pim override-interval *interval-milliseconds*

no ip pim override-interval

default ip pim override-interval

Parameter Description

Parameter	Description
<i>interval-milliseconds</i>	In the range from 1 to 65,535 in the unit of milliseconds

Defaults

The default is 2,500 milliseconds.

Command Mode

Interface configuration mode

Usage Guide

Configuring the override-interval is to set the pruning veto time for the interface.

Configuration Examples

The following example sets the override-interval to 3,000 milliseconds.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim override-interval 3000
```

Related

Command	Description
---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

5.7 ip pim propagation-delay

Use this command to reconfigure the propagation-interval of the hello message.

Use the **no** or **default** form of this command to restore the default setting.

ip pim propagation-delay *interval-milliseconds*

no ip pim propagation-delay

default ip pim propagation-delay

Parameter Description	Parameter	Description
	<i>interval-milliseconds</i>	Propagation-interval of the hello message in the range from 1 to 32,767 in the unit of milliseconds

Defaults The default is 500 milliseconds.

Command Mode Interface configuration mode

Usage Guide Configuring the propagation-delay is to set the transmission delay time for the interface.

Configuration Examples The following example sets the propagation-delay to 600 milliseconds.

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim propagation-delay 600
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.8 ip pim query-interval

Use this command to reconfigure the interval of sending the hello message.

Use the **no** or **default** form of this command to restore the default setting.

ip pim query-interval *interval-seconds*

no ip pim query-interval
default ip pim query-interval

**Parameter
Description**

Parameter	Description
<i>interval-seconds</i>	Interval of sending the hello message in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 30 seconds.

**Command
Mode** Interface configuration mode

Usage Guide If hello interval is set, the hello holdtime value will be updated to 3.5 times of hello interval.

Configuration The following example sets the interval of sending the hello message to 123 seconds.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim query-interval 123
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

5.9 ip pim state-refresh disable

Use this command to prohibit the interface from processing and forwarding the PIM-DM state refresh messages.

Use the **no** or **default** form of this command to restore the default setting.

ip pim state-refresh disable
no ip pim state-refresh disable
default ip pim state-refresh disable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults By default, the PIM-DM state refresh messages can be processed and forwarded.

**Command
Mode** Global configuration mode

Usage Guide When the state refresh function is disabled, the PIM-DM state refresh message is not processed and forwarded. The sent Hello message does not contain the status refresh option. Consequently, the SR Cap field will not be processed when the Hello message is received.

Generally, it is not recommended to disable the status refresh function because disabling this function may converge the PIM-DM multicast forwarding tree again that has been converged, resulting in unnecessary waste of bandwidth and oscillation of multicast routing table.

Configuration The following example disables the processing of the PIM-DM state refresh message.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim state-refresh disable
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.10 ip pim state-refresh origination-interval

Use this command to set the interval of sending the PIM-DM state refresh message. The interval is the seconds elapsed between two state refresh messages.

Use the **no** or **default** form of this command to restore the default setting.

ip pim state-refresh origination-interval *interval-seconds*

no ip pim state-refresh origination-interval

default ip pim state-refresh origination-interval

Parameter Description

Parameter	Description
<i>interval-seconds</i>	Interval of sending the PIM-DM update message in the range from 1 to 100 in unit of seconds

Defaults The default is 60 seconds.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the interval of sending the PIM-DM state refresh message to 65 seconds.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim state-refresh origination-interval 65
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

5.11 show ip pim dense-mode interface

Use this command to display the information about the PIM-DM interface.

show ip pim dense-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	Interface type and interface ID
	detail	Displays details of the interface.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information about the PIM-DM interface.

```
Ruijie# show ip pim dense-mode interface
Address  Interface  VIFIndex  Ver/Mode  Nbr
Mode Count
10.10.10.10 FastEthernet 0/45 3 v2/D 1
50.50.50.50 VLAN4      2 v2/D 1
```

Field	Description
Address	Primary IP address of the PIM-DM interface
Interface	Name of the PIM-DM interface
VIF Index	VIF ID (ID)
Ver/Mode	PIM version/mode
Nbr Count	Number of neighbors of the PIM-DM interface.

Related Commands	Command	Description
	show ip pim dense-mode	Displays the information about the neighbors of

neighbor	the PIM-DM interface.
-----------------	-----------------------

Platform N/A

Description

5.12 show ip pim dense-mode mroute

Use this command to display the information about the PIM-DM routing table.

show ip pim dense-mode mroute [*group-or-source-address* [*group-or-source-address*]]
[**summary**]

Parameter Description	Parameter	Description
	<i>group-or-source-address</i>	Group address or source address
	<i>group-or-source-address</i>	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.
	summary	Displays the brief information of routing entries.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the information about the PIM-Dm routing table.

Examples

```
Ruijie# show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
(1.1.1.111, 229.1.1.1)
MRT lifetime expires in 205 seconds
RPF Neighbor: 50.50.50.1, Nexthop:50.50.50.1,VLAN 4
Upstream IF: VLAN 4
Upstream State: Pruned, PLT:200
Assert State: NoInfo
Downstream IF List:
FastEthernet 0/45:
Downstream State: NoInfo
Assert State: Loser, AT:170
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.13 show ip pim dense-mode neighbor

Use this command to display the information about the PIM-DM neighbors.

show ip pim dense-mode neighbor [*interface-type interface-number*]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the information about the PIM-DM neighbors.

Examples

```
Ruijie# show ip pim dense-mode neighbor
Neighbor-Address Interface      Uptime/Expires    Ver
10.10.10.1    FastEthernet 0/45 00:19:29/00:01:21 v2
50.50.50.1    VLAN 4          00:22:09/00:01:39 v2
```

Description of fields in the results:

Field	Description
Neighbor-Address	IP address of the neighbor
Interface	Name of the interface connecting the neighbor
Uptime/Expires	Valid time and aging time of the entry
Ver	PIM version

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.14 show ip pim dense-mode nexthop

Use this command to display the information about the PIM-DM next hop.

show ip pim dense-mode nexthop

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the information about the PIM-Dm next hop:

Examples

```
Ruijie# show ip pim dense-mode nexthop
Destination Nexthop Nexthop Nexthop Metric Pref
              Num      Addr      Interface
1.1.1.111    1        50.50.50.1 VLAN 4    0      1
```

Field	Description
Destination	Multicast source IP address
Nexthop Num	Number of next hop
Nexthop Addr	IP address of next hop
Nexthop interface	Interface connecting to the of next hop
Metric	Route metric
Pref	Route priority

Related Commands	Command	Description
		N/A

Platform N/A

Description

5.15 show ip pim dense-mode track

Use this command to display the statistics of the PIM-DM packets.

show ip pim dense-mode track

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the clear ip pim dense-mode track every time.

Configuration The following example displays the statistics of the PIM-DM packets.

Examples

```
Ruijie# show ip pim dense-mode track
          PIM packet counters
Elapsed time since counters cleared: 00:04:03
          received      sent
Valid PIMDM packets:      1          8
Hello:                    1          8
Join/Prune:               0          0
Graft:                    0          0
Graft-Ack:                0          0
Assert:                   0          0
State-Refresh:            0          0
PIM-SM-Register:         0          0
PIM-SM-Register-Stop:    0          0
PIM-SM-BSM:              0          0
PIM-SM-C-RP-ADV:         0          0
Unknown Type:             0
Errors:
Malformed packets:       0
Bad checksums:           0
Unknown PIM version:     0
Send errors:              0
```

Related Commands

Command	Description
clear ip pim dense-mode track	Clears the statistics of the PIM packets.

Platform Description N/A

6 PIM-SM Commands

6.1 clear ip pim sparse-mode bsr rp-set *

Use this command to clear all the RP information learnt dynamically.

clear ip pim sparse-mode bsr rp-set *

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide All the RP information learnt dynamically can be cleared manually.

Configuration Examples The following example clears all the RP information learnt dynamically.

```
Ruijie# clear ip pim sparse-mode bsr rp-set *
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.2 clear ip pim sparse-mode track

Use this command to reconfigure the start time of the statistics and clear the PIMv6 packet counter.

clear ip pim sparse-mode track

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to reconfigure the start time of the statistics and clear the PIM packet counter.

Configuration Examples The following example clears the PIM packet counter.

```
Ruijie# clear ip pim sparse-mode track
```

Related Commands

Command	Description
show ip pim sparse-mode track	Displays the PIM packet statistics.

Platform Description N/A

6.3 ip pim accept-bsr list

Use this command to confine the BSR address range.

Use the **no** or **default** form this command to restore the default setting.

ip pim accept-bsr list *access-list*

no ip pim accept-bsr

default ip pim accept-bsr

Parameter Description

Parameter	Description
list <i>access-list</i>	IP standard number ACL in the range of 1 to 99, 1300 to 1999 and characters

Defaults By default, the PIMSM router receives all external BSM packets.

Command Mode Global configuration mode

Usage Guide Use this command to limit the range of the legal BSR.

Configuration Examples The following example confines the BSR address range.

```
Ruijie(config)# ip pim accept-bsr list 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.4 ip pim accept-crp list

Use this command to confine the C-RP address range and the multicast group address range it serves.

Use the **no** or **default** form of this command to restore the default setting,

ip pim accept-crp list *access-list*

no ip pim accept-crp

default ip pim accept-crp

Parameter Description	Parameter	Description
	list <i>access-list</i>	IP extension number ACL in the range of 1 to 99, 1300 to 1999 and characters

Defaults By default, the elected BSR receives all external advertisements of candidate RPs.

Command Global configuration mode

Mode

Usage Guide With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.

Configuration Examples The following example confines the C-RP address range and the multicast group address range it serves.

```
Ruijie (config)# ip pim accept-crp list 100
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.5 ip pim accept-crp-with-null-group

Use this command to receive the C-RP-ADV packets whose prefix-count is 0.

Use the **no** or **default** form of this command to restore the default setting.

ip pim accept-crp-with-null-group

no ip pim accept-crp-with-null-group

default ip pim accept-crp-with-null-group

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults By default, the BSR does not receive the C-RP-ADV packets whose prefix-count is 0.

Command Mode Global configuration mode

Usage Guide With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.

Configuration Examples The following example receives the C-RP-ADV packets whose prefix-count is 0.

```
Ruijie (config)# ip pim accept-crp-with-null-group
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.6 ip pim accept-register list

Use this command to confine the address range of the (S,G) entry of the register packets.

Use the **no** or **default** form of this command to restore the default setting.

ip pim accept-register { **list** *access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *access-list*] }

no ip pim accept-register

default ip pim accept-register

Parameter Description	Parameter	Description
	list <i>access-list</i>	
route-map <i>map-name</i>		Uses a route map to define the (S, G) address range.

Defaults The (S, G) address range is not confined by default.

Command Mode Global configuration mode

Usage Guide This command is used to confine the source IP address of register messages on RP.

Configuration The following example confines the source address of register packets on the RP.

Examples

```
Ruijie (config)# ip pim accept-register list 100
Ruijie (config)# access-list 100 permit ip 192.168.195.0 0.0.0.255 225.1.1.1
0.0.0.255
```

Related Commands	Command	Description
		access-list

Platform N/A

Description

6.7 ip pim bsr-border

Use this command to configure the BSR border.

Use the **no** or **default** form of this command to restore the default setting.

ip pim bsr-border

no ip pim bsr-border

default ip pim bsr-border

Parameter Description	Parameter	Description
		N/A

Defaults No BSR border is configured by default.

Command Mode Interface configuration mode

Usage Guide To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.

Configuration The following example sets the BSR border on the interface *g 0/3*

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if- GigabitEthernet 0/3)# ip pim bsr-border
```

Related Commands	Command	Description
		N/A

Platform N/A

Description

6.8 ip pim bsr-candidate

Use this command to configure the C-BSR.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

no ipv6 pim bsr-candidate

default ip pim bsr-candidate

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	Interface type and number
	<i>hash-mask-length</i>	(Optional) HASK mask length configured for electing the RP in the range from 0 to 32, The default is 10.
	<i>priority-value</i>	(Optional) Priority configured for the candidate BSR in the range from 0 to 255. The default is 64.

Defaults No C-BSR is configured by default.

Command Mode Global configuration mode

Usage Guide A PIM-SM domain must contain a unique Bootstrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. This packet contains the address and priority of the BSR.

This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IP address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message.

The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IP address).

Configuration The following example configures the C-BSR.

Examples Ruijie(config)# ip pim bsr-candidate gi 0/3 30 192

Related Commands	Command	Description
	access-list	N/A

Platform N/A

Description

6.9 ip pim dr-priority

Use this command to set the DR priority.

Use the **no** or **default** form of this command to restore the default setting.

ip pim dr-priority *priority-value*

no ip pim dr-priority

default ip pim dr-priority

Parameter Description	Parameter	Description
	<i>priority-value</i>	The larger the value, the higher the priority is. The range is from 0 to 4,294,967,294.

Defaults The default is 1.

Command Interface configuration mode

Mode

Usage Guide To select a DR:

If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices have the same priority, the one of the largest IP address is elected to be the DR.

If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.

Configuration The following example sets the DR priority.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ip pim dr-priority 10000
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.10 ip pim ignore-rp-set-priority

Use this command to ignore the RP priority.

Use the **no** or **default** form of this command to restore the default setting.

ip pim ignore-rp-set-priority

no ip pim ignore-rp-set-priority
default ip pim ignore-rp-set-priority

Parameter Description	Parameter	Description
		N/A

Defaults By default, the C-RP with higher priority is selected.

Command Mode Global configuration mode

Usage Guide This command is used to ignore the priority of the RP.

Configuration Examples The following example ignores the RP priority.

```
Ruijie(config)# ip pim ignore-rp-set-priority
```

Related Commands	Command	Description
		N/A

Platform Description N/A

6.11 ip pim jp-timer

Use this command to set the interval to send the join/prune message.

Use the **no** or **default** form of this command to restore the default setting.

ip pim jp-timer *seconds*

no ip pim jp-timer

default ip pim jp-timer

Parameter Description	Parameter	Description
		<i>seconds</i>

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example sets the interval to send the Join/Prune message to 50 seconds.

Examples Ruijie(config)# ip pim jp-timer 50

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

6.12 ip pim neighbor-filter

Use this command to confine the neighbor address range.

Use the **no** or **default** form of this command to restore the default setting.

ip pim neighbor-filter *access_list*

no ip pim neighbor-filter *access_list*

default ip pim neighbor-filter *access_list*

**Parameter
Description**

Parameter	Description
<i>access_list</i>	Access control list supporting numerical ACL in the range 1 to 99 and name ACL

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Configuration The following example blocks the neighbor address 192.168.1.5.

Examples Ruijie(config)# interface gi 0/3
Ruijie(config-if- GigabitEthernet 0/3)# ip pim neighbor-filter 14
Ruijie(config-if- GigabitEthernet 0/3)# exit
Ruijie(config)# access-list 14 deny 192.168.1.5 0.0.0.255

**Related
Commands**

Command	Description
access-list	N/A

Platform N/A

Description

6.13 ip pim neighbor-tracking

Use this command to disable join restraint on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim neighbor-tracking

no ip pim neighbor-tracking

default ip pim neighbor-tracking

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.

Configuration Examples The following example disables join restraint on the interface.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ip pim neighbor-tracking
```

Related Commands	Command	Description
	ip pim propagation-delay	N/A

Platform Description N/A

6.14 ip pim override-interval


Use this command to set the override-interval on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim override-interval *milliseconds*

no ip pim override-interval

default ip pim override-interval

Parameter Description	Parameter	Description
	<i>interval-milliseconds</i>	In the range from 1 to 65,535 in the unit of milliseconds
Defaults	The default is 2,500 milliseconds.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to set the override-interval for the interface.	
	 Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.	
Configuration Examples	The following example sets the override-interval as 3000 milliseconds.	
	<pre>Ruijie(config)# interface gi 0/3 Ruijie(config-if-GigabitEthernet 0/3)# ip pim override-interval 3000</pre>	
Related Commands	Command	Description
	ip pim propagation-delay	N/A
Platform Description	N/A	

6.15 ip pim probe-interval

Use this command to set the register probe interval.

Use the **no** or **default** form of this command to restore the default setting.


ip pim probe-interval *seconds*

no ip pim probe-interval

default ip pim probe-interval

Parameter Description	Parameter	Description
	<i>interval-seconds</i>	In the range from 1 to 65535 seconds
Defaults	The default is 5 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to set the registration probe time. The DR can send the null registration message	

to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet.

-  The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or otherwise the system triggers an alarm.

Configuration The following example sets the probe time to 6 seconds.

Examples Ruijie(config)# ip pim probe-interval 6

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

6.16 ip pim propagation-delay

Use this command to set the propagation-delay on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim propagation-delay *milliseconds*

no ip pim propagation-delay

default ip pim propagation-delay

**Parameter
Description**


Parameter	Description
<i>milliseconds</i>	In the range from 1 to 32,765 milliseconds

Defaults The default is 500 milliseconds.

Command Interface configuration mode

Mode

Usage Guide Use this command to set the propagation-delay for the interface.

-  Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration The following example sets the propagation delay to 600 milliseconds.

Examples Ruijie(config)# interface gi 0/3
Ruijie(config)# ip pim propagation-delay 600

Related Commands	Command	Description
	<code>ip pim override-interval</code>	N/A
	<code>ip pim neighbor-tracking</code>	N/A

Platform N/A

Description

6.17 ip pim query-interval

Use this command to set the interval to send the hello packets.

Use the **no** or **default** form of this command to restore the default setting.

ip pim query-interval *seconds*

no ip pim query-interval

default ip pim query-interval

Parameter Description	Parameter	Description
		<i>seconds</i>

Defaults The default is 30 seconds.

Command Mode Interface configuration mode

Usage Guide Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18752.

Configuration Examples The following example sets the interval to send the hello packets to 123 seconds.

```
Ruijie(config)# interface gi 0/3
Ruijie(config)# ip pim query-interval 123
```

Related Commands	Command	Description
		N/A

Platform N/A

Description

6.18 ip pim register-checksum-wholepkt

Use this command to calculate the checksum of the whole register packet.

Use the **no** or **default** form of this command to restore the default setting.

ip pim register-checksum-wholepkt [group-list *access-list*]

no ip pim register-checksum-wholepkt [group-list *access-list*]

default ip pim register-checksum-wholepkt [group-list *access-list*]

Parameter Description	Parameter	Description
	<i>access-list</i>	Access-list: access control list supporting numerical ACL in the range from 100 to 199 and from 1300 to 1999 and name ACL. Group-list <i>access-list</i> :all multicast packets use this configuration by default

Defaults By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message

Command Mode Global configuration mode

Usage Guide Some vendors calculate checksum based on the overall registration packets. Ruijie Networks introduces this function for the compatibility with devices of other vendors.

Configuration The following example calculates the checksum of the whole register packet.

Examples

```
Ruijie(config)#ip pim register-checksum-wholepkt group-list 99
Ruijie(config)# access-list 99 permit 225.1.1.1 0.0.0.255
```

Related Commands	Command	Description
	access-list	N/A

Platform N/A
Description

6.19 ip pim register-decapsulate-forward

Use this command to enable the RP to decapsulate the register packets and forward the multicast packets.

Use the **no** or **default** form of this command to restore the default setting.

ip pim register-decapsulate-forward

no ip pim register-decapsulate-forward

default ip pim register-decapsulate-forward

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to implement the decapsulate of the PIM-SM registration packets with the multicast data packets received on the candidate RP and forward the multicast data packets. As the decapsulating and forwarding are performed by the software, it is not recommended to configure this command in the case that many registration packets need to be decapsulated and forwarded, which may cause the CPU busy with this function configured.

Configuration Examples The following example enables the RP to decapsulate the register packets and forwards the multicast packets.

```
Ruijie(config)# ip pim register-decapsulate-forward
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.20 ip pim register-rate-limit

Use this command to limit the rate of register packets.

Use the **no** form of this command to restore the default setting.

ip pim register-rate-limit *rate*

no ip pim register-rate-limit

default ip pim register-rate-limit

Parameter Description	Parameter	Description
	<i>rate</i>	

Defaults By default, there is no rate limitation on register messages.

Command Mode Global configuration mode

Usage Guide This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.

Configuration The following example limits the rate of register packets.

Examples Ruijie(config)# ip pim register-rate-limit 3000

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.21 ip pim register-rp-reachability

Use this command to check RP reachability before sending register packets.

Use the **no** or **default** form of this command to restore the default setting.

ip pim register-rp-reachability

no ip pim register-rp-reachability

default ip pim register-rp-reachability

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the RP reachability is not checked before sending register packets.

Command Global configuration mode

Mode

Usage Guide This command is used to check the RP reachability before sending register packets. If not, register packets are not transmitted.

Configuration Examples The following example checks the RP reachability before sending register packets.

Ruijie(config)# ipv6 pim register-rp-reachability

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.22 ip pim register-source

Use this command to specify the source IP address of the register packets.

Use the **no** or **default** form of this command to restore the default setting.

ip pim register-source { *local_address* | *interface-type interface-number* }

no ip pim register-source

default ip pim register-source

Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface whose IP address is used as the source IP address of register packets
	<i>interface-number</i>	
	<i>local_address</i>	Specifies the source IP address of the register packet.

Defaults By default, the source IP address of register packets is the IP address of the DR interface connecting the multicast source.

Command Mode Global configuration mode

Usage Guide This command is used to configure the source IP address of register messages. The source IP address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IP address as the destination IP address of the Register-Stop packet. It is not necessary to enable the PIM.

Configuration The following example specifies the source IP address of the register packets.

Examples

```
Ruijie(config)# ip pim register-source 192.168.195.80
Ruijie(config)# ip pim register-source gi 0/3
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.23 ip pim register-suppression

Use this command to set the register suppression time.

Use the **no** or **default** form of this command to restore the default setting.

ip pim register-suppression *seconds*

no ip pim register-suppression

default ip pim register-suppression

Parameter Description	Parameter	Description
	<i>seconds</i>	Suppression time in the range from 1 to 65,535 in the unit of seconds.

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide Executing this command on the DR will change the register packet suppression time configured. if the **ip pim rp-register-kat** command is not configured, executing this command on RP will modify the period of RP keepalive.

Configuration Examples The following example sets the register suppression time to 100 seconds.

```
Ruijie(config)# ip pim register-suppression 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.24 ip pim rp-address

Use this command to configure the static RP.

Use the **no** or **default** form of this command to restore the default setting.

ip pim rp-address *rp-address* [*access_list*]

no ip pim rp-address *rp-address* [*access_list*]

default ip pim rp-address *rp-address* [*access_list*]

Parameter Description	Parameter	Description
	<i>rp-address</i>	IP address of RP
	<i>access_list</i>	Access control list supporting numerical ACL in the range 1 to 99 and 1300 to 1999 and name ACL. All multicast groups are supported by default.

Defaults No IP address is configured for the static RP by default.

Command Mode Global configuration mode

Usage Guide This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that:

If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence.

You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once.

If there are more than one static RP in a multicast group, the one of the highest IP address is used. Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted.

After configuration is performed, the static RP's source IP address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IP address. When you select a RP from a static RP group, the first entry, namely the one with the largest IP address, will be selected first.

Deleting a static IP address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.

Configuration The following example specifies the source IPv6 address of the register packet.

Examples

```
Ruijie(config)# ip pim rp-address 210.34.0.55 4
Ruijie(config)# access-list 4 permit 255.1.1.1 0.0.0.255
```

**Related
Commands**

Command	Description
access-list	N/A

Platform N/A
Description

6.25 ip pim rp-candidate

Use this command to configure the C-RP.

Use the **no** or **default** form of this command to restore the default setting.

ip pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *seconds*] [**group-list** *access_list*]

no ip pim rp-candidate [*interface-type interface-number*]

default ip pim rp-candidate [*interface-type interface-number*]

**Parameter
Description**

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Interface type and interface number
<i>priority-value</i>	(Optional) Priority in the range 0 to 255, 192 by default
<i>seconds</i>	(Optional) Interval in the range 0 to 16,383 seconds, 60s by default
<i>access_list</i>	(Optional) Numerical ACL in the range 1 to 99 or name ACL. By

	default, all multicast groups are permitted.
--	--

Defaults No C-RP is configured by default.

Command Global configuration mode

Mode

Usage Guide In the PIM-SM protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.

Configuration The following example configures the C-RP.

Examples

```
Ruijie(config)# ip pim rp-candidate gi 0/3 priority 200 group-list 3 interval 70
Ruijie(config)# access-list 3 permit 255.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform N/A

Description

6.26 ip pim rp-register-kat

Use this command to set the KAT interval on the RP.

Use the **no** or **default** form of this command to restore the default setting.

ip pim rp-register-kat *seconds*

no ip pim rp-register-kat

default ip pim rp-register-kat

Parameter Description

Parameter	Description
<i>seconds</i>	KAT timer time in the range from 1 to 65,525 in the unit of seconds

Defaults The default is 210 seconds.

Command Global configuration mode

Mode

Usage Guide This command is used to configure the KAT interval of RP.

Configuration The following example sets the KAT interval on the RP to 250 seconds.

Examples

```
Ruijie(config)# ip pim rp-register-kat 250
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.27 ip pim sparse-mode

Use this command to enable PIM-SM on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim sparse-mode

no ip pim sparse-mode

default ip pim sparse-mode




Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide This command is used to enable PIM-SM on the interface.

-  You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SM. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM.
-  During the execution of this command, if the prompt "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.
-  During the execution of this command, if the prompt "PIM-SM Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SM on the interface, delete the unnecessary PIM-SM, PIM-DM or DVMRP interfaces.

Configuration The following example enables PIM-SM on the interface.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ip pim sparse-mode
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

6.28 ip pim sparse-mode subvlan

Use this command to enable PIM-SM on a super VLAN. Use the **no** form or **default** form of this command to disable PIM-SM on a super VLAN.

ip pim sparse-mode subvlan [all | vid]

no ip pim sparse-mode subvlan

default ip pim sparse-mode subvlan

Parameter Description	Parameter	Description
		all
	<i>vid</i>	Sends packets to a specified sub VLAN.

Defaults PIM-SM is disabled on super VLANs by default.

Command Mode Interface configuration mode

Usage Guide In most scenarios on the PIM network, the PIM SM protocol does not need to be enabled on interfaces of a super VLAN. In general, a super VLAN includes many sub VLANs. If the PIM SM protocol is enabled on the interfaces of the super VLAN, multicast packets will be replicated and sent to all sub VLANs. As a result, traffic generated easily exceeds the device processing capability, causing protocol flapping. In some scenarios that require the PIM SM protocol to be enabled on the interfaces of the super VLAN, the PIM-SM sub VLAN function may be configured, to send packets to a specified sub VLAN or all sub VLANs.

Configuration Examples The following example enables PIM-SM on VLAN 100 to send packets to its sub VLAN 200.

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 100
Ruijie(config-if-vlan 100)# ip pim sparse-mode subvlan 200
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.29 ip pim spt-threshold

Use this command to enable the SPT switching function.

Use the **no** or **default** form of this command to restore the default setting.

ip pim spt-threshold [**group-list** *access-list*]

no ip pim spt-threshold [**group-list** *access-list*]

default ip pim spt-threshold [**group-list** *access-list*]

Parameter Description	Parameter	Description
	<i>access_list</i>	(Optional) Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL. By default, all multicast groups are permitted for SPT switching.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using **group-list**) or all multicast groups (not using **group-list**) .

Configuration Examples The following example enables the SPT switching function.

```
Ruijie(config)# ip pim spt-threshold group-list 12
Ruijie(config)# access-list 12 permit 225.1.1.1 0.0.0.255
```

Related Commands	Command	Description
	access-list	N/A

Platform N/A

Description

6.30 ip pim ssm

Use this command to enable SSM and set the SSM group address range.

Use the **no** or **default** form of this command to restore the default setting.

ip pim ssm { **default** / **range** *access_list* }

no ip pim ssm

default ip pim ssm

Parameter Description	Parameter	Description
	default	Multicast groups of 232/8
	range <i>access_list</i>	Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable PIM-SSM (or in some specific multicast groups).

Configuration Examples The following command enables SSM and sets the SSM group range to 232/8:

```
Ruijie(config)# ip pim ssm default
```

The following command sets the source-specific multicast with ACL 10.

```
Ruijie(config)# ip pim ssm range 10
```

```
Ruijie(config)# access-list 10 permit 232.0.0.1 0.0.0.255
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.31 ip pim triggered-hello-delay

Use this command to configure Triggered-Hello-Delay time on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim triggered-hello-delay *seconds*

no ip pim triggered-hello-delay

default ip pim triggered-hello-delay

Parameter Description	Parameter	Description
	<i>seconds</i>	In the range from 1 to 5 in the unit of seconds.

Defaults The default is 5 seconds.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the

interface sends the Hello message in random time.

Configuration The following command sets the triggered-hello-delay to 3 seconds.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ip pim triggered-hello-delay 3
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.32 show debugging

Use this command to display the debugging status.

show debugging

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to turn on debugging switch.

Configuration The following example displays the debugging status.

Examples

```
Ruijie#show debugging
ip packet debug:
ip packet debug debugging is on, acl: 0
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.33 show ip pim sparse-mode bsr-router

Use this command to display the BSR information

show ip pim sparse-mode bsr-router

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display BSR information.

Configuration Examples The following example displays BSR information.

```
Ruijie# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 192.168.127.1
Uptime: 01d23h14m, BSR Priority: 64, Hash mask length: 10
Next bootstrap message in 00:00:42
Role: Candidate BSR Priority: 64, Hash mask length: 10
State: Elected BSR
Candidate RP: 30.30.100.200(GigabitEthernet 0/3)
Advertisement interval 60 seconds
00:00:32
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.34 show ip pim sparse-mode interface

Use this command to display PIM-SM interface information.

show ip pim sparse-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>interface-type</i> <i>interface-number</i>	(Optional) Interface name. This command takes effect for all interfaces by default.
detail	(Optional) Displays the details of an interface.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command displays the PIM-SM information on the interface.

Configuration The following example displays the PIM-SM information on the interface.

Examples

```
Ruijie#show ip pim sparse-mode interface detail
GigabitEthernet 0/3 (vif 3):
Address 30.30.100.200, DR 30.30.100.200
Hello period 30 seconds, Next Hello in 11 seconds
Triggered Hello period 5 seconds
Neighbors:
2.2.2.2
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

6.35 show ip pim sparse-mode local-members

Use this command to display the local IGMP information on the PIM-SM interface.

show ip pim sparse-mode local-members [*interface-type interface-number*]

Parameter Description

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface name. This command takes effect for all interfaces by default.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command displays the local IGMP information on the PIM-SM interface.

Configuration The following example displays the local IGMP information on the PIM-SM interface.

Examples

```
Ruijie (config-if)#sh ip pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/3:
(*, 225.1.1.1) : Include
Loopback 1:
GigabitEthernet 0/5:
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

6.36 show ip pim sparse-mode mroute

Use this command to display the PIM-SM routing information.

show ip pim sparse-mode mroute [*group-or-source-address* [*group-or-source-address*]] [**proxy**]

**Parameter
Description**

Parameter	Description
<i>group-or-source-address</i>	Group IP address or source IP address. Two addresses cannot both be the group addresses or the source addresses.
proxy	RPF vector information.

Defaults N/A

**Command
Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display routing information. Only one group IP address, one source IP address or one group IP address-source IP address pair can be configured at a time. You can also specify no group IP address or source IP address.

Configuration The following example displays the PIM-SM routing information.

Examples

```
Ruijie#show ip pim sparse-mode mroute
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

6.37 show ip pim sparse-mode neighbor

Use this command to display the neighbor information.

show ip pim sparse-mode neighbor [detail]

Parameter Description	Parameter	Description
	detail	(Optional) Displays the details of an interface.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command displays the information on neighbors.

Configuration Examples The following example displays the neighbor information.

```
Ruijie# show ip pim sparse-mode neighbor
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.38 show ip pim sparse-mode nexthop

Use this command to display the next-hop information, including the interface ID, address and metric.

show ip pim sparse-mode nexthop

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the next-hop information.

```
Ruijie# show ip pim sparse-mode nexthop
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.39 show ip pim sparse-mode rp mapping

Use this command to display the information on all RPs and the multicast groups they serve.

show ip pim sparse-mode rp mapping

Parameter Description

Parameter	Description
<i>mapping</i>	All group and RP information

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information on all RPs and the multicast groups they serve.

```
Ruijie# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 30.30.200.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:00:51, expires: 00:01:39
RP: 30.30.100.1
Info source: 30.30.200.1, via bootstrap, priority 192
Uptime: 00:19:14, expires: 00:01:38
Group(s): 224.0.0.0/4, Static
RP: 100.100.100.100
Uptime: 00:45:35
```

Related Commands

Command	Description
---------	-------------

N/A	N/A
-----	-----

Platform N/A

Description

6.40 show ip pim sparse-mode rp-hash

Use this command to display the RP information corresponding to the group address.

show ip pim sparse-mode rp-hash *group-address*

Parameter Description	Parameter	Description
	<i>group-address</i>	Group address to be resolved

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command displays the RP information corresponding to the group address.

Configuration The following example displays the RP information corresponding to the group address.

Examples

```
Ruijie# show ip pim sparse-mode rp-hash 255.1.1.1
RP: 30.30.100.1
Info source: 30.30.100.1, via bootstrap
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

6.41 show ip pim sparse-mode track

Use this command to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.

show ip pim sparse-mode track

Parameter Description	Parameter	Description

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the **clear ip pim sparse-mode track** every time.

Configuration Examples The following example displays the number of sent and received PIM packets during the period from the beginning of the statistics till now.

```
Ruijie # show ip pim sparse-mode track
PIM packet counters track
Elapsed time since counters cleared: 00:04:03
received    sent
Valid PIMSM packets:    0          8
Hello:                  0          8
Join-Prune:             0          0
Register:               0          0
Register-Stop:         0          0
Assert:                 0          0
BSM:                   0          0
C-RP-ADV:               0          0
PIMDM-Graft:           0
PIMDM-Graft-Ack :      0
PIMDM-State-Refresh:   0
Unknown PIM Type:      0
Errors:
Malformed packets:          0
Bad checksums:              0
Send errors:                0
Packets received with unknown PIM version:    0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7 PIM-SMv6 Commands

7.1 clear ipv6 mroute

Use this command to clear multicast routing entries.

```
clear ipv6 mroute { * | ipv6_group_address [ ipv6_source_address ] }
```

Parameter Description	Parameter	Description
	*	Deletes all the multicast routing entries.
	<i>ipv6_group_address</i>	Deletes the multicast routing entries of the specific group.
	<i>ipv6_source_address</i>	Deletes the multicast routing entries of the specific group and source IPv6 address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all the multicast routing entries.

```
Ruijie# clear ipv6 mroute *
```

The following example clears the multicast routing entries of the specified group.

```
Ruijie# clear ipv6 mroute ff66::6666
```

The following example clears the multicast routing entries of the specified group and source address.

```
Ruijie# clear ipv6 mroute ff66::6666 3333::3333
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.2 clear ipv6 mroute statistics

Use this command to delete the statistics of the multicast routing entries.

```
clear ipv6 mroute statistics { * | ipv6_group_address [ ipv6_source_address ] }
```

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
*	Deletes the statistics of all multicast routing entries.
<i>ipv6_group_address</i>	Deletes the statistics of the multicast routing entries of the specific group.
<i>ipv6_source_address</i>	Deletes the statistics of the multicast routing entries of the specific group and source IPv6 address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example deletes the statistics of the multicast routing entries.

Examples Ruijie# `clear ipv6 mroute statistics *`

The following example clears the statistics of the multicast routing entries of the specified group.

Ruijie# `clear ipv6 mroute statistics ff66::6666`

The following example clears the statistics of the multicast routing entries of the specified group and source address.

Ruijie# `clear ipv6 mroute statistics ff66::6666 3333::3333`

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.3 clear ipv6 pim sparse-mode bsr rp-set *

Use this command to clear the RP information learnt dynamically.

clear ipv6 pim sparse-mode bsr rp-set *

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Only the RP information learnt dynamically can be cleared manually.

Configuration The following example clears the RP information learnt dynamically.

Examples

```
Ruijie# clear ipv6 pim sparse-mode bsr rp-set *
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

7.4 clear ipv6 pim sparse-mode track

Use this command to reconfigure the start time of the statistics and clear the PIMv6 packet counter.

clear ipv6 pim sparse-mode track

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears the PIMv6 packet counter.

Examples

```
Ruijie# clear ipv6 pim sparse-mode track
```

Related Commands	Command	Description
	show ipv6 pim sparse-mode track	N/A

Platform N/A

Description

7.5 ipv6 pim accept-bsr list

Use this command to confine the BSR address range.

Use the **no** or **default** form this command to restore the default setting.

ipv6 pim accept-bsrr list *ipv6_access-list*

no ipv6 pim accept-bsr

default ipv6 pim accept-bsr

Parameter Description	Parameter	Description
		list <i>ipv6_access-list</i>

Defaults By default, the PIM-SMv6 router receives all external BSM packets.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example confines the BSR address range.

```
Ruijie(config)# ipv6 pim accept-bsr list bsr-list
```

Related Commands	Command	Description
		N/A

Platform Description N/A

7.6 ipv6 pim accept-crp list

Use this command to confine the C-RP address range and the multicast group address range it serves.

Use the **no** or **default** form of this command to restore the default setting,

ipv6 pim accept-crp list *ipv6_access-list*

no ipv6 pim accept-crp

default ipv6 pim accept-crp-with-null-group

Parameter Description	Parameter	Description
		list <i>ipv6_access-list</i>

Defaults No address is filtered by default.

Command Mode Global configuration mode

Usage Guide With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.

Configuration The following example confines the C-RP address range and the multicast group address range it serves.

Examples

```
Ruijie (config)# ipv6 pim accept-crp list crp-list
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

7.7 ipv6 pim accept-crp-with-null-group

Use this command to receive the C-RP-ADV packets whose prefix-count is 0.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim accept-crp-with-null-group

no ipv6 pim accept-crp-with-null-group

default ipv6 pim accept-crp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.

Configuration The following example receives the C-RP-ADV packets whose prefix-count is 0.

Examples

```
Ruijie (config)# ipv6 pim accept-crp-with-null-group
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

7.8 ipv6 pim accept-register

Use this command to accept specific register packets at the RP.

Use the **no** or **default** form of this command to restore the default setting.

```
ipv6 pim accept-register { list ipv6_access-list [ route-map map-name ] | route-map map-name
[list ipv6_access-list ] }
```

```
no ipv6 pim accept-register
```

```
default ipv6 pim accept-register
```

Parameter Description	Parameter	Description
	list <i>ipv6_access-list</i>	IPv6 ACL supporting named ACL
	route-map <i>map-name</i>	Defines the routing map rule

Defaults All register packets are received by default.

Command Global configuration mode

Mode

Usage Guide This command is used to confine the source IPv6 address of register messages on RP. If the unauthorized register source is received, the RP will return the Register-Stop message immediately.

Configuration The following example denies register packets of the specified source address at the RP.

Examples

```
Ruijie(config)# ipv6 pim accept-register list register-access-list
Ruijie(config)# ipv6 access-list register-access-list
Ruijie(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
```

Platform N/A

Description

7.9 ipv6 pim bsr-border

Use this command to configure the BSR border.

Use the **no** or **default** form of this command to restore the default setting.

```
ipv6 pim bsr-border
```

```
no ipv6 pim bsr-border
```

```
default ipv6 pim bsr-border
```

Parameter Description	Parameter	Description
	N/A	N/A

Defaults No BSR border is configured by default.

Command Interface configuration mode
Mode

Usage Guide To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.

Configuration The following example sets the BSR border on the interface *gi 0/3*.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet)# ipv6 pim bsr-border
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

7.10 ipv6 pim bsr-candidate

Use this command to configure the candidate bootstrap router (C-BSR).

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

no ipv6 pim bsr-candidate

default ipv6 pim bsr-candidate

**Parameter
Description**

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Interface type and number.
<i>hash-mask-length</i>	(Optional) HASK mask length configured for electing the RP in the range from 0 to 128. The default is 126.
<i>priority-value</i>	(Optional) Priority configured for the C-BSR in the range from 0 to 255. The default is 64.

Defaults No C-BSR is configured by default.

Command Global configuration mode
Mode

Usage Guide A PIM-SMv6 domain must contain a unique Bootstrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM

domain. This packet contains the address and priority of the BSR.

This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IPv6 address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message.

The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IPv6 address).

Configuration The following example s configures the C-BSR.

Examples Ruijie(config)# ipv6 pim bsr-candidate gi 0/3 30 100

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

7.11 ipv6 pim dr-priority

Use this command to configure the DR priority.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority

default ipv6 pim dr-priority

**Parameter
Description**

Parameter	Description
<i>priority-value</i>	The larger the value, the higher the priority is. The range is from 0 to 4,294,967,294. The default is 1.

Defaults The default is 1.

**Command
Mode** Interface configuration mode

Usage Guide To select a DR:

- If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices have the same priority, the one of the largest IP address is elected to be the DR.
- If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.

Configuration The following example configures the DR priority.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if)# ipv6 pim dr-priority 11234
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.12 ipv6 pim ignore-rp-set-priority

Use this command to ignore the RP priority.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim ignore-rp-set-priority
no ipv6 pim ignore-rp-set-priority
default ipv6 pim ignore-rp-set-priority

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the C-RP with a higher priority is selected.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example ignores the RP priority.

Examples

```
Ruijie(config-if)# ipv6 pim ignore-rp-set-priority
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.13 ipv6 pim jp-timer

Use this command to set the interval to send the join/prune message.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim jp-timer *seconds*

no ipv6 pim jp-timer

default ipv6 pim jp-timer

Parameter Description	Parameter	Description
	<i>seconds</i>	Interval to send the join/prune message in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide This command is used to set the interval to send the Join/Prune message.

Configuration Examples The following example sets the interval to send the Join/Prune message to 100 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim jp-timer 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.14 ipv6 pim neighbor-filter

Use this command to confine the neighbor address range.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim neighbor-filter *ipv6_access-list*

no ipv6 pim neighbor-filter *ipv6_access-list*

default ipv6 pim neighbor-filter *ipv6_access-list*

Parameter Description	Parameter	Description
	<i>ipv6_access_list</i>	IPv6 ACL supporting named ACL

- Defaults** This function is disabled by default.
- Command Mode** Interface configuration mode
- Usage Guide** Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Configuration Examples The following example blocks the neighbor address fe80::2d0:f8ff:fe22:33ad.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if- GigabitEthernet 0/3)# ipv6 pim neighbor-filter acl
Ruijie(config-if- GigabitEthernet 0/3)# exit
Ruijie(config)# ipv6 access-list acl
Ruijie(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
```

Related Commands

Command	Description
ipv6_access-list	N/A

Platform Description N/A

7.15 ipv6 pim neighbor-tracking

Use this command to disable join restraint on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim neighbor-tracking

no ipv6 pim neighbor-tracking

default ipv6 pim neighbor-tracking

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join

message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.

Configuration The following example disables join restraint on the interface.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet)# ipv6 pim neighbor-tracking
```

**Related
Commands**

Command	Description
ipv6 pim propagation-delay	N/A

Platform

N/A

Description

7.16 ipv6 pim override-interval

Use this command to set the override-interval on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim override-interval *milliseconds*

no ipv6 pim override-interval

default ipv6 pim override-interval

**Parameter
Description**

Parameter	Description
<i>milliseconds</i>	In the range 1 to 65,535 in the unit of milliseconds

Defaults


The default is 2,500 milliseconds.

**Command
Mode**

Interface configuration mode

Usage Guide

Use this command to set the override-interval for the interface.

 Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration

The following example sets the override-interval to 3,000 milliseconds.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet)# ipv6 pim override-interval 3000
```

**Related
Commands**

Command	Description
ipv6 pim propagation-delay	N/A

Platform N/A

Description

7.17 ipv6 pim probe-interval

Use this command to set the register probe interval.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim probe-interval *seconds*

no ipv6 pim probe-interval

default ipv6 pim probe-interval


Parameter Description	Parameter	Description
	<i>seconds</i>	In the range from 1 to 65,535 in the unit of seconds

Defaults The default is 5 seconds.

Command Global configuration mode

Mode

Usage Guide Use this command to set the registration probe time. The DR can send the null registration message to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet.

-  The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or otherwise the system triggers an alarm.

Configuration The following example sets the probe time as 6 seconds.

Examples Ruijie(config)# ipv6 pim probe-interval 6

Related Commands	Command	Description
	ipv6 pim register-suppression	N/A

Platform N/A

Description

7.18 ipv6 pim propagation-delay

Use this command to set the propagation-delay on the interface.

Use the **no** or **default** form of this command to restore the default setting.


ipv6 pim propagation-delay *milliseconds*
no ipv6 pim propagation-delay
default ipv6 pim propagation-delay

Parameter Description	Parameter	Description
	<i>milliseconds</i>	In the range from 1 to 32,765 in the unit of milliseconds

Defaults The default is 500 milliseconds.

Command Mode Interface configuration mode

Usage Guide Use this command to set the propagation-delay for the interface.

 Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration Examples The following example sets the propagation delay to 600 milliseconds.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim propagation-delay 600
```

Related Commands	Command	Description
	ipv6 pim override-interval	N/A
	ipv6 pim neighbor-tracking	N/A

Platform Description N/A

7.19 ipv6 pim query-interval

Use this command to set the interval to send the hello packets.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim query-interval *seconds*
no ipv6 pim query-interval
default ipv6 pim query-interval

Parameter Description	Parameter	Description
	<i>seconds</i>	Interval to send the Hello message in the range from 1 to 65,535 in the unit of seconds

- Defaults** The default is 30.
- Command Mode** Interface configuration mode
- Usage Guide** Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18725.

Configuration Examples The following example sets the interval to send the hello packets.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim query-interval 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.20 ipv6 pim register-checksum-wholepkt

Use this command to calculate the checksum of the whole register packet.
 Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim register-checksum-wholepkt [group-list *ipv6_access-list*]
no ipv6 pim register-checksum-wholepkt [group-list *ipv6_access-list*]
default ipv6 pim register-checksum-wholepkt [group-list *ipv6_access-list*]

Parameter Description

Parameter	Description
group-list <i>ipv6_access-list</i>	IPv6 ACL supporting named ACL. <i>ipv6_access-list</i> :all multicast packets use this configuration by default

Defaults By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message.

Command Mode Global configuration mode

Usage Guide Some vendors calculate checksum based on the overall registration packets. Ruijie Networks introduces this function for the compatibility with these vendors.

Configuration Examples The following example calculates the checksum of the whole register packet.

```
Ruijie(config)#ipv6 pim register-checksum-wholepkt group-list
```

```
checksum-access-list
Ruijie(config)# ipv6 access-list 99 checksum-access-list
Ruijie(config-ipv6-acl)# permit ipv6 any ff66::6666/64
```

**Related
Commands**

Command	Description
ipv6 access-list	N/A

Platform N/A
Description

7.21 ipv6 pim register-rate-limit

Use this command to limit the rate of register packets.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim register-rate-limit *rate*

no ipv6 pim register-rate-limit

default ipv6 pim register-rate-limit

**Parameter
Description**

Parameter	Description
<i>rate</i>	Maximum number of register packets that can be sent per second, in the range from 1 to 65,535.

Defaults By default, there is no rate limitation on register messages.

**Command
Mode** Global configuration mode

Usage Guide This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.

Configuration The following example limits the rate of register packets.

Examples Ruijie(config)# ipv6 pim register-rate-limit 3000

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

7.22 ipv6 pim register-rp-reachability

Use this command to check RP reachability before sending register packets.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim register-rp-reachability

no ipv6 pim register-rp-reachability

default ipv6 pim register-rp-reachability

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the RP reachability is not checked before sending register packets.

Command Mode Global configuration mode

Usage Guide This command is used to check the RP reachability before transmission. If not, register packets are not transmitted.

Configuration Examples The following example checks the RP reachability before sending register packets.

```
Ruijie(config)# ipv6 pim register-rp-reachability
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.23 ipv6 pim register-source

Use this command to specify the source IPv6 address in the register packets.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim register-source { *ipv6_local_address* | *interface-type interface-number* }

no ipv6 pim register-source

default ipv6 pim register-source

Parameter Description	Parameter	Description
	<i>ipv6_local_address</i>	Source IPv6 address of register packets
	<i>interface-type</i> <i>interface-number</i>	Interface whose IPv6 address is used as the source IPv6 address of register packets

Defaults By default, the source IPv6 address of register packets is the IPv6 address of the DR interface connecting the multicast source.

Command Mode Global configuration mode

Usage Guide This command is used to configure the source IPv6 address of register messages. The source IPv6 address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IPv6 address as the destination IPv6 address of the Register-Stop packet.

 It is not necessary to enable the PIM-SMv6 on the associated interfaces.

Configuration The following example configures the source IPv6 address of register messages.

Examples

```
Ruijie(config)# ipv6 pim register-source 3333::3333
Ruijie(config)# ipv6 pim register-source gi 0/3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.24 ipv6 pim register-suppression

Use this command to set the register suppression time.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim register-suppression *seconds*

no ipv6 pim register-suppression

default ipv6 pim register-suppression

Parameter Description

Parameter	Description
<i>seconds</i>	Suppression time in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide Executing this command on the DR will change the register packet suppression time configured. if the `ipv6 pim rp-register-kat` command is not configured, executing this command on RP will modify the

period of RP keepalive.

Configuration The following example sets the register packet suppression time.

Examples

```
Ruijie(config)# ipv6 pim register-suppression 100
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

7.25 ipv6 pim rp embedded

Use this command to enable the embedded RP function.

Use the **no** or **default** form of this command to disable this function.

ipv6 pim rp embedded [group-list *ipv6_acl_name*]

no ipv6 pim rp embedded

default ipv6 pim rp embedded

Parameter Description	Parameter	Description
		group-list <i>ipv6_acl_name</i>

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the embedded RP function explicitly and to enable the embedded RP for the IPv6 multicast address of specified embedded RP address.

Configuration Examples The following example enables the embedded RP for the IPv6 multicast addresses of all embedded RP addresses.

```
Ruijie(config)# ipv6 pim rp embedded
```

Related Commands	Command	Description
		ipv6 access-list

Platform N/A

Description

7.26 ipv6 pim rp-address

Use this command to configure the static RP.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access_list*]

no ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access-list*]

default ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access-list*]

Parameter Description	Parameter	Description
	<i>ipv6_rp-address</i>	IPv6 address of RP
	<i>ipv6_access_list</i>	IPv6 ACL supporting named ACL

Defaults No IPv6 address is configured for the static RP by default.

Command Global configuration mode

Mode

Usage Guide This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that:

- If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence.
- You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once.
- If there are more than one static RP in a multicast group, the one of the highest IPv6 address is used.
- Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted.
- After configuration is performed, the static RP's source IPv6 address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IPv6 address. When you select a RP from a static RP group, the first entry, namely the one with the largest IPv6 address, will be selected first.

Deleting a static IPv6 address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.

Configuration The following example configures the RP static address.

```
Ruijie(config)# ipv6 pim rp-address 3333::3333 acl
Ruijie(config)# ipv6 access-list acl
Ruijie(config)# permit ipv6 any ff66::6666/64
```

Related Commands	Command	Description
	ipv6 access-list	N/A

Platform N/A
Description

7.27 ipv6 pim rp-candidate

Use this command to configure the candidate RP (C-RP).

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *ipv6_access-list*]

no ipv6 pim rp-candidate [*interface-type interface-number*]

default ipv6 pim rp-candidate [*interface-type interface-number*]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	Interface type and interface number
	<i>priority-value</i>	(Optional) Priority in the range from 0 to 255, 192 by default
	<i>interval-seconds</i>	(Optional) Interval in the range from 0 to 16383 in the unit of seconds, 60 by default
	<i>ipv6_access_list</i>	(Optional) IPv6 ACL supporting named ACL

Defaults N/A

Command Mode Global configuration mode

Usage Guide In the PIM-SMv6 protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL.

Note that the group range is calculated only based on the permit rule, not the deny rule.

Configuration Examples The following example configures the RP candidate.

```
Ruijie(config)# ipv6 pim rp-candidate gi 0/3 priority 200 group-list acl
interval 40
Ruijie(config)# ipv6 access-list acl
Ruijie(config-ipv6-acl)# permit ipv6 any ff66::6666/64
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.28 ipv6 pim rp-register-kat

Use this command to set the Keepalive Timer (KAT) of a (S, G) entry created by the register packet at the RP.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim rp-register-kat *seconds*

no ipv6 pim rp-register-kat

default ipv6 pim rp-register-kat

Parameter	Parameter	Description
Description	<i>seconds</i>	KAT value in the range from 1 to 65,525 in the unit of seconds.

Defaults The default is equal to the sum of register probe time and three times register suppression time.

Command Global configuration mode
Mode

Usage Guide The KAT value at the RP should be greater than three times the register suppression time at the source DR. Otherwise, the KAT will end and the entry (S,G) will time out before another register packet is sent, so that multicast stream will break down in a short while.

Configuration The following example configures the KAT interval of RP.

Examples Ruijie(config)# `ipv6 pim rp-register-kat 250`

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.29 ipv6 pim sparse-mode

Use this command to enable PIM-SMv6 on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim sparse-mode

no ipv6 pim sparse-mode







default ipv6 pim sparse-mode

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to enable PIM-SMv6 on the interface.

-  You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SMv6. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM.
-  During the execution of this command, if the prompt "Failed to enable PIM-SMv6 on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.
-  During the execution of this command, if the prompt "PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SMv6 on the interface, delete the unnecessary PIM-SMv6, or PIM-DMv6 interfaces.
-  If the interface is of tunnel-type, only 6Over4 configuration tunnel, 6Over GRE tunnel, 6Over4 configuration tunnel and 6Over6 GRE tunnel support the IPv6 multicasting at the moment. The multicasting can also be enabled on other tunnel interfaces which do not support the multicasting, but no error message will be displayed and no multicast packets will be received and forwarded.
-  The multicast tunnel can only be built on the Ethernet interface, the nested tunnel and the multicast data Qos/ACL are not supported.
-  IPv6 multicast packets cannot be forwarded through SuperVLAN.

Configuration The following example enables PIM-SMv6 on the interface.

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim sparse-mode
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.30 ipv6 pim sparse-mode subvlan

Use this command to enable PIM-SMv6 on a super VLAN. Use the no form or default form of this command to disable PIM-SMv6 on a super VLAN.

ipv6 pim sparse-mode subvlan [**all** | *vid*]

no ipv6 pim sparse-mode subvlan

default ipv6 pim sparse-mode subvlan

Parameter Description	Parameter	Description
	all	Sends packets to all sub VLANs.
	<i>vid</i>	Sends packets to a specified sub VLAN.

Defaults PIM-SMv6 is disabled on super VLANs by default.

Command Mode Interface configuration mode

Usage Guide In most scenarios on the PIM network, the PIM SMv6 protocol does not need to be enabled on interfaces of a super VLAN. In general, a super VLAN includes many sub VLANs. If the PIM SMv6 protocol is enabled on the interfaces of the super VLAN, multicast packets will be replicated and sent to all sub VLANs. As a result, traffic generated easily exceeds the device processing capability, causing protocol flapping. In some scenarios that require the PIM SMv6 protocol to be enabled on the interfaces of the super VLAN, the PIM-SMv6 sub VLAN function may be configured, to send packets to a specified sub VLAN or all sub VLANs.

Configuration Examples The following example enables PIM-SMv6 on VLAN 100 to send packets to its sub VLAN 200.

```
Ruijie# configure terminal
Ruijie(config)# interface vlan 100
Ruijie(config-if-vlan 100)# ipv6 pim sparse-mode subvlan 200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.31 ipv6 pim spt-threshold

Use this command to enable SPT switch.

Use the **no** or **default** form of this command to restore the default setting.

```

ipv6 pim spt-threshold [group-list ipv6_access-list ]
no ipv6 pim spt-threshold [ group-list ipv6_access-list ]
default ipv6 pim spt-threshold [ group-list ipv6_access-list ]

```

Parameter Description	Parameter	Description
	<i>ipv6_access_list</i>	(Optional) IPv6 ACL supporting named ACL

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using group-list) or all multicast groups (not using group-list) .

Configuration The following example enables the SPT switch.

```

Examples
Ruijie(config)# ipv6 pim spt-threshold acl
Ruijie(config)# ipv6 access-list acl
Ruijie(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad /128
ff66::6666/64

```

Related Commands	Command	Description
	ipv6 access-list	N/A

Platform Description N/A

7.32 ipv6 pim ssm

Use this command to enable SSM and set the SSM group address range.

Use the **no** or **default** form of this command to restore the default setting.

```

ipv6 pim ssm { default | range ipv6_access-list }
no ipv6 pim ssm
default ipv6 pim ssm

```

Parameter Description	Parameter	Description
	default	Group in the range of FF3x::/32
	range <i>ipv6_access_list</i>	IPv6 ACL supporting named ACL

Defaults This function is disabled by default.

Command Global configuration mode
Mode

Usage Guide This command is used to enable PIM-SSMv6 (or in some specific multicast groups).

Configuration The following example sets the source-specific multicast of the multicast group range ACL.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim ssm range acl
Ruijie(config-ipv6-acl)# permit ipv6
fe80::2d0:f8ff:fe22:33ad /128 ff32::3333/64
```

**Related
Commands**

Command	Description
ipv6 access-list	N/A

Platform N/A
Description

7.33 ipv6 pim static-rp-preferred

Use this command to configure a higher priority for static RP over the C-RP.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim static-rp-preferred

no ipv6 pim static-rp-preferred

default ipv6 pim static-rp-preferred

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults By default, the priority of the RP elected through BSR mechanism is high than the one configured statically.

Command Interface configuration mode
Mode

Usage Guide With this command configured, the priority of the static RP is higher than the one elected through the BSR mechanism.

Configuration The following example configures the priority of the static RP is higher than the one elected through the BSR mechanism.

Examples

```
Ruijie(config-if)# ipv6 pim static-rp-preferred
```

**Related
Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

Platform N/A
Description

7.34 ipv6 pim triggered-hello-delay

Use this command to configure Triggered-Hello-Delay time on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 pim triggered-hello-delay *seconds*

no ipv6 pim triggered-hello-delay

default ipv6 pim triggered-hello-delay

Parameter Description	Parameter	Description
	<i>seconds</i>	In the range from 1 to 5 in the unit of seconds.

Defaults The default is 5 seconds.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message at the random time.

Configuration Examples The following example sets the triggered-hello-delay to 3 seconds.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim triggered-hello-delay 3
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.35 show debugging

Use this command to display the debugging status.

show debugging

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the debugging status.

Examples

```
Ruijie # show debugging
PIM-SM Debugging status:
PIM packet debugging is on.
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.36 show ipv6 pim sparse-mode bsr-router

Use this command to display the BSR information.

show ipv6 pim sparse-mode bsr-router

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Privileged EXEC mode/Global configuration mode /Interface configuration mode

Command Mode Privileged EXEC mode/ global configuration mode / interface configuration mode

Usage Guide N/A

Configuration The following example displays BSR information.

Examples

```
Ruijie# show ipv6 pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 3333::8888
Uptime:00:03:31, BSR Priority: 64, Hash mask length: 126
```



```

Next bootstrap message in 00:00:47
Role: Candidate BSR Priority: 64, Hash mask length: 126
State: Elected BSR
Candidate RP: 3333::8888(GigabitEthernet 0/5)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:37

```

Related Commands

Command	Description
N/A	N/A

Platform N/A**Description**

7.37 show ipv6 pim sparse-mode interface

Use this command to display PIM-SMv6 interface information.

show ipv6 pim sparse-mode interface [*interface-type interface-number*] [**detail**]

Parameter Description

Parameter	Description
<i>interface-type</i>	(Optional) Interface name. This command takes effect for all interfaces by default.
<i>interface-number</i>	(Optional) Displays the details of an interface.
detail	(Optional) Displays the details of an interface.

Defaults N/A**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode**Usage Guide** N/A**Configuration** The following example displays the PIM-SMv6 interface information.**Examples**

```

Ruijie #show ipv6 pim sparse-mode interface detail
GigabitEthernet 0/5 (vif 1):
Address fe80::2d0:f8ff:fe22:33ad, DR fe80::2d0:f8ff:fe22:34b3
Hello period 30 seconds, Next Hello in 6 seconds
Triggered Hello period 5 seconds
Secondary addresses:
    3333::8888
    4444::4444
Neighbors:
    fe80::2d0:f8ff:fe22:34b3

```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.38 show ipv6 pim sparse-mode local-members

Use this command to display the local MLD information on the PIM-SMv6 interface.

show ipv6 pim sparse-mode local-members [*interface-type interface-number*]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	(Optional) Interface name. This command takes effect for all interfaces by default.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the local MLD information on the PIM-SMv6 interface.

Examples

```
Ruijie (config-if)#show ipv6 pim sparse-mode local-members
PIM Local membership information
GigabitEthernet 0/5:
  (*, ff66::6666) : Include
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.39 show ipv6 pim sparse-mode mroute

Use this command to display the PIM-SMv6 routing information.

show ipv6 pim sparse-mode mroute [*group-or-source-address* [*group-or-source-address*]]

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	<i>group-or-source-address</i>	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display route information. Only one group IPv6 address, one source IPv6 address or one group IPv6 address-source IPv6 address pair can be configured at a time. You can also specify no group IP address or source IPv6 address.

Configuration Examples N/A

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

7.40 show ipv6 pim sparse-mode neighbor

Use this command to display the neighbor information.

show ipv6 pim sparse-mode neighbor [detail]

Parameter Description	Parameter	Description
	detail	(Optional) Displays the details of an interface.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command displays the information on neighbors.

Configuration Examples The following example displays the neighbor information..

```
Ruijie# show ipv6 pim sparse-mode neighbor detail
Nbr fe80::2d0:f8ff:fe22:34b3 (GigabitEthernet 0/5)
Expires in 86 seconds
Secondary addresses:
```

```
6666::6666
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.41 show ipv6 pim sparse-mode nexthop

Use this command to display the next hop information, including the interface ID, address and metric.

show ipv6 pim sparse-mode nexthop

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

7.42 show ipv6 pim sparse-mode rp mapping

Use this command to display the information on all RPs and the multicast groups they serve.

show ipv6 pim sparse-mode rp mapping

Parameter Description	Parameter	Description
	mapping	All groups and RP information.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the information on all RPs and the multicast groups they serve.

Examples

```
Ruijie# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 3333::1
    Info source: 3333::1, via bootstrap, priority 192
    Uptime: 00:12:40, expires: 00:01:50
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

7.43 show ipv6 pim sparse-mode rp-hash

Use this command to display the RP information corresponding to the group address.

show ipv6 pim sparse-mode rp-hash *ipv6-group-address*

Parameter Description

Parameter	Description
<i>ipv6_group-address</i>	IPv6 group address

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the RP information corresponding to the group address..

Examples

```
Ruijie# show ipv6 pim sparse-mode rp-hash ff66::6666
RP: 3333::8888
Info source: 3333::8888, via bootstrap
```

```
PIMv2 Hash Value 126
RP 3333::8888, via bootstrap, priority 192, hash value 1468234650
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A**Description**

7.44 show ipv6 pim sparse-mode track

Use this command to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.

show ipv6 pim sparse-mode track

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A**Command
Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIMv6 packet counter is cleared on calling the clear ipv6 pim sparse-mode track every time.

**Configuration
Examples** The following example displays the number of sent and received PIM packets during the period from the beginning of the statistics till now.

```
Ruijie# show ipv6 pim sparse-mode track
PIMv6 packet counters track
Elapsed time since counters cleared: 00:04:03
                received      sent
Valid PIMSMv6 packets:    0          8
Hello:                    0          8
Join-Prune:                0          0
Register:                  0          0
Register-Stop:             0          0
Assert:                    0          0
BSM:                       0          0
C-RP-ADV:                  0          0
```

```

PIMDMv6-Graft:          0
PIMDMv6-Graft-Ack:     0
PIMDMv6-State-Refresh: 0
Unknown PIMv6 Type:    0
Errors:
Malformed packets:          0
Bad checksums:              0
Send errors:                0
Packets received with unknown PIMv6 version: 0
    
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

8 IGMP Snooping Commands

8.1 clear ip igmp snooping gda-table

Use this command to clear the Group Destination Address (GDA) table.

clear ip igmp snooping gda-table

Parameter Description	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the clear ip igmp snooping gda-table command.				
Configuration Examples	The following example clears the Group Destination Address (GDA) table. <pre>Ruijie# clear ip igmp snooping gda-table</pre>				
Platform Description	N/A				

8.2 clear ip igmp snooping statistics

Use this command to clear IGMP Snooping statistics.

clear ip igmp snooping statistics

Parameter Description	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	This command is used to clear the IGMP Snooping statistics, which can be displayed by using the show ip igmp snooping statistics command.				

Configuration The following example clears the IGMP Snooping statistics.

Examples Ruijie# clear ip igmp snooping statistics

Platform N/A

Description

8.3 deny

Use this command to deny the forwarding of the multicast streams in the range specified by the profile.

deny

Parameter Description

Parameter	Description
N/A	N/A

Defaults The forwarding of the multicast streams in the range specified by the profile is denied.

Command Mode Profile configuration mode

Usage Guide First, configure the multicast range using the range command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Configuration Examples The following is an example of deny the forwarding of the multicast stream 224.2.2.2 to 224.2.2.244.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# deny
```

Platform N/A

Description

8.4 ip igmp profile

Use this command to create a profile and enter the IGMP profile configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

default ip igmp profile *profile-number*

Parameter

Parameter	Description
-----------	-------------

Description		
	<i>profile-number</i>	Profile number, in the range from 1 to 1024
Defaults	No profile is created by default.	
Command Mode	Global configuration mode	
Usage Guide	<p>The profile is a filter to permit/deny specified groups in the following steps:</p> <ul style="list-style-type: none"> ● Use the ip igmp profile command to create a profile and enter profile configuration mode. ● Use the range command to define a profile range. ● Use the permit command to permit this profile in the filtering, or use the deny command to deny this profile in the filtering. ● If the deny command is used without any profile specified, all profiles in the profile are permitted. ● If the permit command is used without any profile specified, all profiles in the profile are denied. 	
Configuration Examples	<p>The following example creates and permits profile 1 with addresses from 224.2.2.2 to 224.2.2.244.</p> <pre>Ruijie(config)# ip igmp profile 1 Ruijie(config-profile)# range 224.2.2.2 224.2.2.244 Ruijie(config-profile)# permit</pre>	
Platform	N/A	
Description		

8.5 ip igmp snooping

Use this command to enable IGMP snooping and enter the IVGL mode.

ip igmp snooping ivgl

Use this command to enable IGMP snooping and enter the SVGL mode.

ip igmp snooping svgl

Use this command to enable IGMP snooping and enter the IVGL-SVGL mode.

ip igmp snooping ivgl-svgl

Use the no or default command to restore the default setting.

no ip igmp snooping

default ip igmp snooping

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	IGMP Snooping is disabled by default.	
Command Mode	Global configuration mode	

Usage Guide

- **IVGL (Independent VLAN Group Learning):** In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in the same VLAN.
- **SVGL (Shared VLAN Group Learning):** In this mode, the hosts in different VLANs share the same multicast flow. A host can request multicast flows across VLANs. By designating a Shared VLAN, you can only forward the multicast flows received in this Shared VLAN to other member ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast address range, within which the multicast flow can be forwarded across VLANs. By default, all group range is not within the SVGL range and all multicast flows are dropped. As shown in Figure-3:
- **IVGL-SVGL mode:** also known as promiscuous mode. In this mode, the IVGL mode and the SVGL mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across VLANs and without which the member ports are forwarded in the same VLAN.



SVGL mode and IVGL-SVGL mode conflict with the IP multicast function.



PIM Snooping must depend on either IVGL or IVGL-SVGL mode of IGMP Snooping. Use **no ip igmp snooping** command to disable IGMP Snooping after PIM Snooping is disabled.

Configuration

The following example enables IGMP Snooping and enters the IVGL mode.

Examples

```
Ruijie(config)# ip igmp snooping ivgl
```

The following example enables IGMP Snooping and enters the SVGL mode.

```
Ruijie(config)# ip igmp snooping svgl
Ruijie(config)# ip igmp snooping svgl profile 1
```

The following example enables IGMP Snooping and enters the IVGL-SVGL mode.

```
Ruijie(config)# ip igmp snooping ivgl-svgl
Ruijie(config)# ip igmp snooping svgl profile 1
```

Platform

N/A

Description

8.6 ip igmp snooping dyn-mr-aging-time

Use this command to set the aging time of a dynamic routing interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping dyn-mr-aging-time *seconds*

no ip igmp snooping dyn-mr-aging-time

default ip igmp snooping dyn-mr-aging-time

Parameter Description	Parameter	Description
		seconds

Defaults The default is 300 seconds.

Command Mode Global configuration mode

Usage Guide If a dynamic routing interface does not receive IGMP query packets or PIM hello packets before aged, this interface will be deleted.

When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.

Configuration Examples The following example sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.

```
Ruijie(config)# ip igmp snooping dyn-mr-aging-time 100
```

Platform Description N/A

8.7 ip igmp snooping fast-leave enable

Use this command to enable the fast leave function.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping fast-leave enable

no ip igmp snooping fast-leave enable

default ip igmp snooping fast-leave enable

Parameter Description	Parameter	Description
		N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message.

Subsequently, when the system receives a specific group query packet, the system does not forward it to the corresponding interface. Leave packets include IGMPv2 leave packets and

IGMPv3 report packets of the include type without source addresses. The fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.

Configuration The following example enables the fast leave function.

Examples

```
Ruijie(config)# ip igmp snooping fast-leave
```

Platform N/A

Description

8.8 ip igmp snooping filter

Use this command to specify the profile for ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping filter *profile-number*

no ip igmp snooping filter *profile-number*

default ip igmp snooping filter

Use this command to specify the profile for VLANs.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping vlan *vlan-id filter profile-number*

no ip igmp snooping vlan *vlan-id filter*

default ip igmp snooping vlan *vlan-id filter*

Parameter Description

Parameter	Description
<i>profile-number</i>	Profile number from 1 to 1024

Defaults This function is disabled by default.

Command Mode Global configuration mode/Interface configuration mode

Usage Guide A specific profile must be created before association.

Configuration The following example specifies profile 1 for interface fastEthernet 0/1.

Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

Platform N/A

Description

8.9 ip igmp snooping host-aging-time

Use this command to configure the aging time of IGMP dynamic ports.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping host-aging-time *seconds*

no ip igmp snooping host-aging-time

default ip igmp snooping host-aging-time

Parameter	Parameter	Description
Description	<i>seconds</i>	Aging time. The unit is second. The value ranges from 1 to 65,535.

Defaults The default is 260 seconds.

Command Mode Global configuration mode

Usage Guide The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group. When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by **host-aging-time**. If the timer expires, the system determines that there is no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the **ip igmp snooping host-aging-time** command is executed, the aging time will be determined by **host-aging-time**. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.

Configuration The following example sets the aging time to 30 seconds.

Examples Ruijie(config)# ip igmp snooping host-aging-time 30

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.10 ip igmp snooping l2-entry-limit

Use this command to set the maximum number of multicast groups.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping l2-entry-limit *number*

no ip igmp snooping l2-entry-limit

default ip igmp snooping l2-entry-limit

Parameter	Parameter	Description
-----------	-----------	-------------

Description	<i>number</i>	Number of multicast groups. The value ranges from 0 to 65,536.				
Defaults	The default is 65,536.					
Command Mode	Global configuration mode					
Usage Guide	The maximum number of multicast groups includes the multicast groups in all ports of all VLANs (including dynamic and static multicast groups). When the number of multicast groups reaches the limit, learning new group records and configuring new static multicast group ports are not allowed.					
Configuration Examples	The following example sets the maximum number of multicast groups to 2000.					
Examples	<pre>Ruijie(config)# ip igmp snooping l2-entry-limit 2000</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show ip igmp snooping</td> <td>Displays the maximum number of multicast groups.</td> </tr> </tbody> </table>	Command	Description	show ip igmp snooping	Displays the maximum number of multicast groups.	
Command	Description					
show ip igmp snooping	Displays the maximum number of multicast groups.					
Platform Description	N/A					

8.11 ip igmp snooping limit-ipmc

Use this command to add a multicast source IP address check entry.

Use the **no** or **default** form of this command is used to delete a source IP checklist entry.

ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

no ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

default ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID
	<i>group-address</i>	Multicast group address
	<i>source-address</i>	Multicast source IP address

Defaults Only source IP address check is enabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to filter the multicast packets. With it enabled, all multicast packets from illegal IP addresses will be discarded.

 Source IP address check and multicast routing function cannot be enabled meanwhile.

Configuration steps:

1. Enable source IP address check and specify the source IP address.
2. (Optional) Specify the multicast group address and source IP address for a specific VLAN.

Configuration The following example enables source address check to receive multicast packets only from 192.168.1.10 and allows packets into VLAN 203 and VLAN 104 from (192.168.1.10 , 229.1.1.1).

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping source-check default-server 192.168.1.10
Ruijie(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server
192.168.1.10
Ruijie(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server
192.168.1.10
Ruijie(config)# end
```

Platform N/A

Description

8.12 ip igmp snooping max-groups

Use this command to configure the maximum number of groups that can be added dynamically to this interface.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

default ip igmp snooping max-groups

Parameter	Parameter	Description
Description	<i>number</i>	The maximum group number from 0 to 1,024

Defaults No maximum group number is configured by default.

Command Mode Interface configuration mode

Usage Guide If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this interface is beyond the range.

Configuration The following example configures the maximum number of multicast groups to 100 on the megabit interface 0/1:

Examples

```
Ruijie(config)# interface Ethernet 0/1
Ruijie(config-if)# ip igmp snooping max-group 100
```

Platform N/A

Description

8.13 ip igmp snooping mrouter learn pim-dvmrp

Use this command to configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface

Use the **no** form of this command to disable the dynamic learning.

Use the **default** form of this command to restore the default setting.

ip igmp snooping mrouter learn pim-dvmrp

no ip igmp snooping mrouter learn pim-dvmrp

default ip igmp snooping [vlan *vid*] mrouter learn pim-dvmrp

Parameter Description	Parameter	Description
	vlan <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide Routing interface is a port through which a multicast device (with IGMP Snooping enabled) is directly connected to a multicast neighbouring device (with multicast routing protocols enabled). By default, the dynamic routing interface learning function is enabled. You can use the no form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled. When the source port check function is enabled, only the multicast flow enters from the routing interface is legal and it is forwarded to the registered interface by the multicast equipment, the multicast flow from the non routing interface is considered to be the illegal and is discarded. With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.

Configuration The following example enables the dynamic routing interface learning function on VLAN 1.

Examples

```
Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

Platform N/A

Description

8.14 ip igmp snooping preview

Use this command to allow the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.

Use **no** or **default** form of this command to disable multicast preview.

ip igmp snooping preview *profile-number*

no ip igmp snooping preview

default ip igmp snooping preview

Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number (1-1024)

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Apply the IGMP Profile to a multicast preview function. When the user doesn't have access to the multicast streams (namely the user might be filtered by IGMP Snooping filter), it can allow the user to preview partial contents. This function shall be used in conjunction with IGMP Snooping filter or multicast control in order to realize effective multicast preview.

Configuration Examples The following example associates the profile 2 to the Ethernet 0/1 and associates multicast preview with profile 1.

```
Ruijie(config)# ip igmp snooping preview 1
Ruijie(config-if)# int Ethernet 0/1
Ruijie(config-if)# ip igmp snooping filter 2
```

Platform N/A

Description

8.15 ip igmp snooping preview interval

Use this command to configure the interval that allows the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.

Use **no** or **default** form of this command to restore the default setting.

ip igmp snooping preview interval *seconds*

no ip igmp snooping preview interval

default ip igmp snooping preview interval

Parameter Description	Parameter	Description
	<i>seconds</i>	Preview interval from 1 to 300 in the unit of seconds

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide	N/A
Configuration Examples	The following example sets the multicast preview interval as 100 seconds on the 100M port of 0/1: <pre>Ruijie(config)# ip igmp snooping preview 1 Ruijie(config)# ip igmp snooping preview interval 100</pre>
Platform	N/A
Description	

8.16 ip igmp snooping querier

Use this command to enable the IGMP querier.

Use **no** or **default** form of this command to restore the default setting.

ip igmp snooping querier

no ip igmp snooping querier

default ip igmp snooping [vlan *vid*] querier

Parameter Description	Parameter	Description
	vlan <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function.
If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.

Configuration Examples The following example enables the IGMP querier function in VLAN 2.

```
Ruijie(config)# ip igmp snooping querier
Ruijie(config)# ip igmp snooping vlan 2 querier
```

Platform N/A
Description

8.17 ip igmp snooping querier address

Use this command to specify a source IP address for IGMP querier.

Use **no** or **default** form of this command to remove the source IP address configured.

ip igmp snooping [vlan *vid*] querier address *a.b.c.d*

no ip igmp snooping [vlan *vid*] querier address

default ip igmp snooping [vlan *vid*] querier address

Parameter Description	Parameter	Description
	vlan vid	VLAN ID. By default, the specified version is supported on all VLANs.
	<i>a.b.c.d</i>	Source IP address of the IGMP querier
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	<p>After enabling IGMP querier, you must configure a source IP address for the IGMP querier to activate this function.</p> <p>If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.</p>	
Configuration Examples	<p>The following example specifies the source IP of the IGMP querier as 1.1.1.1 on the device.</p> <pre>Ruijie(config)# ip igmp snooping querier address 1.1.1.1</pre> <p>The following example specifies the source IP of the IGMP querier as 1.1.1.1 in VLAN 3.</p> <pre>Ruijie(config)# ip igmp snooping vlan 3 querier address 1.1.1.1</pre>	
Platform Description		

8.18 ip igmp snooping querier max-response-time

Use this command to configure the maximum response time of the IGMP querier.

Use **no** or **default** form of this command to restore to the default setting.

ip igmp snooping [vlan vid] querier max-response-time seconds

no ip igmp snooping [vlan vid] querier max-response-time

default ip igmp snooping [vlan vid] querier max-response-time

Parameter Description	Parameter	Description
	<i>num</i>	Maximum response time from 1 to 25 in the unit of seconds
	vlan vid	VLAN ID. By default, the specified version is supported on all VLANs.
Defaults	The default is 10 seconds.	
Command Mode	Global configuration mode	
Usage Guide	<p>Configure this command to specify the maximum response time to query packets.</p> <p>By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.</p>	

Configuration	The following example specifies the maximum response time of the IGMP querier on the device.
Examples	<pre>Ruijie(config)# ip igmp snooping querier max-response-time 15</pre> <p>The following example specifies the maximum response time of the IGMP querier in VLAN 3.</p> <pre>Ruijie(config)# ip igmp snooping vlan 3 querier max-response-time 15</pre>
Platform	N/A
Description	

8.19 ip igmp snooping querier query-interval

Use this command to specify the interval for IGMP querier to send query packets.

Use **no** or **default** form of this command to restore the default setting.

ip igmp snooping querier query-interval *seconds*

no ip igmp snooping querier query-interval

default ip igmp snooping [vlan *vid*] querier query-interval

Parameter Description	Parameter	Description
	<i>seconds</i>	Query interval from 1 to 18,000 in the unit of seconds
	vlan <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration The following example configures the query interval on the device.

Examples

```
Ruijie(config)# ip igmp snooping querier query-interval 100
```

The following example configures the query interval in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier query-interval 100
```

Platform N/A

Description

8.20 ip igmp snooping querier timer expiry

Use this command to specify the expiration timer for non-querier.

Use **no** form of this command to restore the default setting.

ip igmp snooping [vlan *vid*] querier timer expiry *seconds*

ip igmp snooping [vlan *vid*] querier timer expiry *seconds*

default ip igmp snooping [vlan *vid*] querier timer expiry

Parameter Description	Parameter	Description
	<i>seconds</i>	The expiration timer from 60 to 300 in the unit of seconds
	vlan <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults The default is 125 seconds.

Command Mode Global configuration mode

Usage Guide After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier.
If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples The following example configures the non-querier expiration timer on the device.

```
Ruijie(config)# ip igmp snooping querier timer expiry 60
```

The following example configures the non-querier expiration timer in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

Platform Description N/A

8.21 ip igmp snooping querier version

Use the following commands to specify IGMP Snooping querier version.

ip igmp snooping [vlan *vid*] querier version 1

ip igmp snooping [vlan *vid*] querier version 2

ip igmp snooping [vlan *vid*] querier version 3

Use **no** or **default** form of this command to restore to the default setting.

no ip igmp snooping [vlan *vid*] querier version

default ip igmp snooping [vlan *vid*] querier version

Parameter Description	Parameter	Description
	vlan <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults The default version is IGMPv2.

Command Mode Global configuration mode

Usage Guide IGMPv1, IGMPv2 and IGMPv3 are supported.
If an IGMP querier version has been configured in a VLAN, the version specified in the VLAN will be used first.

Configuration The following example configures IGMP querier version on the device.

Examples

```
Ruijie(config)# ip igmp snooping querier version 1
```

Platform N/A

Description

8.22 ip igmp snooping query-max-response-time

Use this command to specify the time for the switch to wait for the member join message after receiving the **query** message.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-resposne-time

default ip igmp snooping query-max-response-time

**Parameter
Description**

Parameter	Description
<i>seconds</i>	The aging time of the routing interface that the switch learns dynamically, in the range from 1 to 65.535

Defaults The default is 10 seconds.

Command Mode Global configuration mode

Usage Guide You can specify the time for the switch to wait for the member join message after receiving the query message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member.

This command lets you adjust the waiting time after receiving the query message. This command takes effect only after the switch receives the next member join message. This command does not change the current wait time.

**Configuration
Examples** The following examples sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.

```
Ruijie(config)# ip igmp snooping query-max-response-time 100
```

Platform N/A

Description

8.23 ip igmp snooping source-check default-server

Use this command to enable the source IP address check to permit one or several IPMC flows

from the server of the specified IP address.

Use the **no** or **default** form of this command is used to restore the default setting.

ip igmp snooping source-check default-server *source-address*

no ip igmp snooping source-check


default ip igmp snooping source-check

Parameter Description	Parameter	Description
	<i>source-address</i>	Default multicast source IP address

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The source IP address check function takes effect globally. Once it is enabled, only the IPMC streams from the specified IP address are permitted.

 Source IP address check and IP multicast function cannot work meanwhile.

The device allows users to configure the source IP address of all IPMC streams, called default multicast server. The default server must be set as long as the source IP address check function is enabled.

Configuration The following example enables the multicast source IP address check function.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping source-check default-server 192.168.1.10
Ruijie(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server
192.168.1.10
Ruijie(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server
192.168.1.10
Ruijie(config)# end
```

Platform N/A

Description

8.24 ip igmp snooping source-check port

Use this command to enable the source port check function of IGMP Snooping.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping source-check port

no ip igmp snooping source-check port

default ip igmp snooping source-check port

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The source port check function is used to permit one or several IPMC flows from the mroute port. When it is enabled, only the IPMC streams from the specified port are permitted. When it is disabled, all the IPMC streams are permitted and forwarded.

Configuration Examples The following example enables the source port check function of IGMP Snooping.

```
Ruijie(config)# ip igmp snooping source-check port
```

Platform N/A

Description

8.25 ip igmp snooping suppression enable

Use this command to enable IGMP snooping suppression.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping suppression enable

no ip igmp snooping suppression enable

default ip igmp snooping suppression enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide When this function is enabled, IGMP Snooping only forwards the first report from a specific VLAN or group, and suppresses the following reports to constrain traffic in the networks. This function is only supported on IGMPv1 and IGMPv2 reports.

Configuration Examples The following example enables IGMP snooping suppression on the device.

```
Ruijie(config)# ip igmp snooping suppression enable
```

Platform N/A

Description

8.26 ip igmp snooping svgl profile

Use this command to specify the multicast group address range applied in the SVGL/IVGL-SVGL mode.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping svgl profile *profile-number*

no ip igmp snooping svgl profile

default ip igmp snooping svgl profile

Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number, in the range of 1-1,024

Defaults No profile is associated.

Command Mode Global configuration mode

Usage Guide When the IGMP Snooping works in the SVGL and IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode. That is to say, the member ports of the multicast forwarding entry can be forwarded across the VLANs while the member ports of the multicast forwarding entry in the other multicast address range must belong to the same VLAN.

Configuration Examples The following example specifies the profile 2 applied in SVGL mode.

```
Ruijie(config)# ip igmp snooping svgl profile 2
```

Platform N/A

Description

8.27 ip igmp snooping svgl subvlan

Use this command to specify the subvlan of multicast VLAN.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping svgl subvlan [*vid-range*]

no ip igmp snooping svgl subvlan [*vid-range*]

default ip igmp snooping svgl subvlan [*vid-range*]

Parameter Description	Parameter	Description
	<i>vid-range</i>	VLAN ID or range of VLAN ID

Defaults By default, all VLANs except shared VLANs serve as its sub VLANs.

Command Mode	Global configuration mode
Usage Guide	This command only takes effect in SVGL and IVGL-SVGL mode.
Configuration Examples	The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs. <pre>Ruijie(config)# ip igmp snooping svgl vlan 3 Ruijie(config)# ip igmp snooping svgl subvlan 2,5-7</pre>
Platform	N/A
Description	

8.28 ip igmp snooping svgl vlan

Use this command to specify the shared VLAN in SVGL mode.

Use the **no** form of this command to restore the default setting.

ip igmp snooping svgl vlan *vid*

no ip igmp snooping svgl vlan

default ip igmp snooping svgl vlan

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID

Defaults By default , the shared VLAN is VLAN 1.

Command Mode Global configuration mode

Usage Guide This command only works in the SVGL and IVGL-SVGL mode.

Configuration Examples The following example specifies the vlan2 as the shared vlan
The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs.

```
Ruijie(config)# ip igmp snooping svgl vlan 3
Ruijie(config)# ip igmp snooping svgl subvlan 2,5-7
```

Platform N/A

Description

8.29 ip igmp snooping tunnel

Use this command to enable 802.1Q tunneling (QinQ) support for IGMP Snooping.

Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping tunnel
no ip igmp snooping tunnel
default ip igmp snooping tunnel

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled.

Command Mode Global configuration mode

Usage Guide After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways:

- First: QinQ transmits IGMP packets transparently. Create multicast entries in the VLAN to which the IGMP packets belong, and forward IGMP packets in the VLAN.
- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of Port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed by Port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10.
- Second: Create multicast entries in the default VLAN to which the dot1q-tunnel ports belong, and forward multicast packets in the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port.
- For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed Port A. When multicast requests of VLAN 10 are sent to Port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1. By default, the second way is used.

Configuration The following example enables QinQ support for IGMP Snooping.

Examples Ruijie(config)# ip igmp snooping tunnel

Platform N/A

Description

8.30 ip igmp snooping vlan

Use this command to enable the IGMP Snooping in the specified VLAN and enter IVGL mode.

Use the **no** form of this command is used to disable the IGMP Snooping.

Use the **default** form of this command to restore the default setting.

ip igmp snooping vlan *vid*
no ip igmp snooping vlan *vid*

default ip igmp snooping vlan *vid***Parameter
Description**

Parameter	Description
<i>vid</i>	VLAN ID in the range from 1 to 4,094

Defaults


IGMP Snooping is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable or disable the IGMP snooping on the specified vlan.

 The PIM Snooping in the specified VLAN works only when IGMP Snooping is configured. To disable PIM Snooping, you must disable IGMP Snooping in the VLAN first, or disabling will fail and be prompted.

Configuration

The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 2.

Examples

```
Ruijie(config)# ip igmp snooping ivgl
Ruijie(config)# no ip igmp snooping vlan 2
```

Platform

N/A

Description

8.31 ip igmp snooping vlan mrouter interface

Use this command to configure a static routing interface.

Use the **no** form of this command to delete a static routing interface.

Use the **default** form of this command to restore the default setting.

ip igmp snooping vlan *vid mrouter interface interface-type interface-number*

no ip igmp snooping vlan *vid mrouter interface interface-type interface-number*

default ip igmp snooping vlan *vid mrouter interface interface-type interface-number*

**Parameter
Description**

Parameter	Description
<i>vid</i>	VLAN ID in the range from 1 to 4,094
<i>interface-type</i> <i>interface-number</i>	Interface ID

Defaults

No static routing interface is configured by default.

Command Mode

Global configuration mode

Usage Guide

A dynamic routing interface is learned dynamically through IGMP Snooping. A static routing interface is configured by using this command and cannot age.

When an interface is configured as a static routing interface, all multicast streams received on this interface will be forwarded.

When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.

Configuration The following example configures a static routing interface.

Examples

```
Ruijie(config)# ip igmp snooping vlan 1 mrout erinterface fastEthernet 0/1
```

Platform N/A

Description

8.32 ip igmp snooping vlan static interface

Use this command to configure a static member interface of a multicast group.

Use the **no** form of this command to delete a static member interface from a multicast group.

Use the **default** form of this command to restore the default setting.

ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type* *interface-number*
no ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type* *interface-number*
default ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type*
interface-number

Parameter Description

Parameter	Description
<i>vid</i>	VLAN ID in the range from 1 to 4,094
<i>ip-addr</i>	Multicast IP address
<i>interface-id</i>	Interface ID

Defaults No static member interface of any multicast group is configured by default.

Command Mode Global configuration mode

Usage Guide The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

Configuration The following example configures a static member interface for the multicast group 224.1.1.1.

Examples

```
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/1
```

Platform N/A

Description

8.33 permit

Use this command to permit the multicast forwarding for specified ranges of a specified profile.

permit

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The forwarding of the multicast streams in the range specified by the profile is denied.

Command Mode Profile configuration mode

Usage Guide A profile is used to filter a group of multicast packets, so as to assist other features.
Configuration steps:

1. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
2. Use the **range** command to define a range for the profile.
3. Use the **permit** command to permit the multicast forwarding for the profile.

Configuration Examples The following example permits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244 of profile 1.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# permit
```

Platform N/A

Description

8.34 range

Use this command to define a range for a specific profile.

Use the **no** form of the command to remove the range from the profile.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter Description	Parameter	Description
	<i>low-ip-address</i>	Start address of a range
	<i>high-ip-address</i>	End address of a range

Defaults No range is defined for a profile by default.

Command Mode Profile configuration mode

- Usage Guide** A profile is used to filter a group of multicast packets, so as to assist other features.
- Configuration steps:
1. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
 2. Use the **range** command to define a range for the profile.
 3. Use the **permit** command to permit the multicast forwarding for the profile.

Configuration Examples The following is an example of allowingpermits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244: of profile 1.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244224.2.2.2
Ruijie(config-profile)# permit
```

Platform N/A

Description

8.35 show ip igmp profile

Use this command to display the profile information.

show ip igmp profile

show ip igmp profile *profile-number*

Parameter Description	Parameter	Description
	<i>profile-number</i>	Displays configuration information of the designated profile.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the profile information.

Configuration Examples The following example displays the profile information.

```
Ruijie(config-if)# show ip igmp profile
Profile 1
Permit
range 224.0.1.0, 239.255.255.255
```

8.36 show ip igmp snooping

Use this command to display related information of IGMP Snooping.

show ip igmp snooping [**gda-table** | **interfaces** *interface-type interface-number* | **mdevice** | **statistics** [**vlan** *vlan-id*] | **querier** [**detail** | **vlan** *vid*]

Parameter Description	Parameter	Description
	vlan <i>vid</i>	VLAN ID. By default, IGMP Snooping information of all VLANs are displayed.
	<i>interface-type</i> <i>interface-number</i>	Interface type and number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays global IGMP Snooping information.

Examples

```
Ruijie#show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2
IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
The following example displays VLAN1 IGMP Snooping information.
Ruijie#show ip igmp snooping vlan 1
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Global IGMPv2 Fast-Leave :Disable
Global multicast router learning mode :Enable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
-----
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disable
```

```
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

Platform N/A
Description

9 MLD Snooping Commands

9.1 clear ipv6 mld snooping gda-table

Use this command to clear the forwarding table information learned dynamically.

clear ipv6 mld snooping gda-table

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the forwarding table information learned dynamically.

Configuration The following example clears the forwarding table information learned dynamically:

Examples Ruijie# clear ipv6 mld snooping gda-table

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.2 clear ipv6 mld snooping statistics

Use this command to clear the MLD Snooping statistics, including the entry number, the entry volume, the number of various received packets, the group information and the interface information of the corresponding group.

clear ipv6 mld snooping statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use the **show ipv6 mld snooping statistics** command to verify the configuration.

Configuration Examples The following example clears the MLD Snooping statistics.

```
Ruijie# clear ipv6 mld snooping statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.3 deny

Use this command to prevent the multicast flow profile within the specified range from being forwarded in the profile configuration mode.

deny

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The default profile action is **deny**.

Command Mode Profile configuration mode

Usage Guide Profile is a kind of group “filter” that can be referred to by other functions.
 Configuration Steps:
 1. Use the ipv6mld profile command to create a profile and enter the profile mode.
 2. Use the range command to define a group.
 3. Use the permit command to allow this group to pass the filtering; Use the deny command to filter the packets of this group. The default command is deny.

Configuration Examples The following example prevents the multicast flow profile within the range from FF15::1 to FF15::100 from being forwarded.

```
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)# range FF15::1 FF15::100
Ruijie(config-profile)# deny
```

Related	Command	Description
---------	---------	-------------

Commands	
ipv6 mld profile	Creates one profile.
range	Sets the multicast address range.
permit	Sets the profile action permit.

Platform N/A

Description

9.4 ipv6 mld profile

Use the following command to create a profile.

Use the **no** or **default** form of this command to delete a profile.

ipv6 mld profile *profile-number*

no ipv6 mld profile *profile-number*

default ipv6 mld profile *profile-number*

Parameter	Parameter	Description
Description	<i>profile-number</i>	Profile number, in the range from 1 to 1024.

Defaults N/A

Command Global configuration mode

Mode

Usage Guide Profile is a kind of group “filter” that can be referred to by other functions.
 Configuration Steps:

1. Use the **ipv6mld** profile command to create a profile and enter the profile mode.
2. Use the **range** command to define a group.
3. Use the **permit** command to allow this group to pass the filtering; Use the deny command to filter the packets of this group. The default command is deny.

Configuration Examples The following example creates profile 1 and allows the packets sent by devices with MAC address ranging from FF15::1 to FF15::100 to pass the filtering.

```
Ruijie(config)#ipv6 mld profile 1
Ruijie(config-profile)#range FF15::1 FF15::100
Ruijie(config-profile)#permit
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

9.5 ipv6 mld snooping

Use this command to enable MLD Snooping and specify IVGL/SVGL/IVGL-SVGL mode.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping {ivgl | svgl | ivgl-svgl}

no ipv6 mld snooping [ivgl | svgl | ivgl-svgl]

default ipv6 mld snooping [ivgl | svgl | ivgl-svgl]

Parameter Description	Parameter	Description
	ivgl	MLD Snooping is running IVGL mode.
	svgl	MLD Snooping is running SVGL mode.
	ivgl-svgl	MLD Snooping is running IVGL-SVGL mode.

Defaults This function is disabled by default.

Command Global configuration mode

Mode

- Usage Guide**
- In IVGL mode, multicast flow in each VLAN is independent. The host only requests multicast flow from the routing interface within the same VLAN. The device forwards the multicast flow from any VLAN to the member port within the same VLAN.
 - In SVGL mode, multicast flow is shared among VLANs. The host can request multicast flow across VLANs. Shared VLAN (VLAN 1 by default) should be specified. Only multicast flow from Shared VLAN can be forwarded to all member ports within the group address range, which may belong to different VLANs. Profile is used to specify a group range for SVGL. Only multicast flow within this range can be forwarded across VLANs. The other multicast flow is discarded.
 - In IVGL-SVGL mode, Profile is used to specify a group range for SVGL. Multicast flow within this range is in SVGL mode and the other multicast flow is in IVGL mode.
 - IPv6 multicast packets cannot be forwarded through SuperVLAN.

Configuration The following example enables MLD Snooping IVGL mode.

Examples Ruijie(config)# ipv6 igmp snooping ivgl

The following example enables MLD Snooping SVGL mode and specifies the shared VLAN and SVGL group range as VLAN1 and profile1 respectively.

Ruijie(config)# ipv6 igmp snooping svgl

Ruijie(config)# ipv6 igmp snooping svgl profile 1

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

9.6 ipv6 mld snooping dyn-mr-aging-time

Use this command to set the aging time of the dynamic multicast route port.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping dyn-mr-aging-time second

no ipv6 mld snooping dyn-mr-aging-time

default ipv6 mld snooping dyn-mr-aging-time


Parameter Description	Parameter	Description
	<i>second</i>	Sets the aging time of the dynamic multicast route port, in the range from 1 to 3,600 in the unit of seconds.

Defaults The default is 300 seconds.

Command Mode Global configuration mode.

Usage Guide The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the ipv6 PIM Hello packets within the aging timeout on this interface.

Use this command to change the aging time of the routing ports learned dynamically. If the aging time is too short, routing ports will be added and deleted frequently.

 By default, the dynamic learning of routing ports is enabled. If learning fails, use the show run command to check whether this function is enabled.

Configuration Examples The following example sets the aging time of the dynamic multicast routing port to 100 seconds.

```
Ruijie(config)# ipv6 mld snooping dyn-mr-aging-time 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.7 ipv6 mld snooping fast-leave enable

Use this command to enable the MLD Snooping fast-leave function.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping fast-leave enable
no ipv6 mld snooping fast-leave enable
default ipv6 mld snooping fast-leave enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide The interface fast leave is that when IPv6 MLD Leave packets sent from the host are received on an interface, the interface is removed from the outgoing interface list of the corresponding forwarding entry. Then, the switch will not forward the received IPv6 MLD specific group query packets to the interface.



If there is only one receiver connected with the interface, enable the interface fast leave function to save the bandwidth and resources.

Configuration Examples The following example enables mld snooping fast-leave.

```
Ruijie(config)# ipv6 mld snooping fast-leave
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.8 ipv6 mld snooping filter

Use this command to filter the specific multicast flows.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping filter *profile-number*
no ipv6 mld snooping filter
default ipv6 mld snooping filter

Parameter Description	Parameter	Description
	<i>profile-number</i>	Sets the profile number in the range from 1 to 1024.

Defaults This function is disabled by default.

Command Interface configuration mode
Mode

Usage Guide You can configure an MLD Profile on an interface. If the MLD Report packets are received on the interface, the layer-2 device will determine whether the multicast address to be joined the interface is within the allowed range of the MLD Profile. The specified profile must be created before using this command.

Configuration The following example associates profile1 with the interface GigabitEthernet 0/1.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 mld snooping filter 1
```

Related Commands	Command	Description
		ipv6 mld profile

Platform N/A
Description

9.9 ipv6 mld snooping host-aging-time

Use this command to set the aging time of the dynamic member port.

Use the **no** form of this command to cancel this configuration.

Use the **default** form of this command to restore the default setting.

ipv6 mld snooping host-aging-time *seconds*

no ipv6 mld snooping host-aging-time

default ipv6 mld snooping host-aging-time

Parameter Description	Parameter	Description
		<i>seconds</i>

Defaults The default aging time of the dynamic member port is 260 seconds.

Command Global configuration mode
Mode

Usage Guide The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the IPv6 PIM Hello packets within the aging timeout on this interface.

When the MLD Snooping is enabled, the port that receives the MLD Report packet will learn to be a dynamic member port. The default aging time of such dynamic member port is 260 seconds. You can

use this command to adjust the aging time. This configuration takes effect after the port receives the the next Report packet. The aging time of the dynamic member port should be longer than the query interval.

Configuration The following example sets the aging time of the dynamic member port to 30 seconds:

Examples

```
Ruijie(config)# ipv6 mld snooping host-aging-time 30
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

9.10 ipv6 mld snooping max-groups

Use this command to set the maximum group allowed to join the interface dynamically.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping max-groups *number*

no ipv6 mld snooping max-groups

default ipv6 mld snooping max-groups

Parameter Description	Parameter	Description
	<i>number</i>	The number of groups, in the range from 0 to 65,536

Defaults The default is 65,536.

Command Mode Interface configuration mode

Usage Guide With this command configured, when the group number exceeds the specified range on the interface, the switch will not receive and deal with the MLD Report packets.

The multicast groups are counted based on VLANs of an interface. If the interface has 3 VLANs, the counting result is 3 instead of 1 when an FF15::100 multicast request is received by all the VLAN.

Configuration Examples The following example sets the maximum 100 multicast group on the interface GigabitEthernet 0/1.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 mld snooping max-groups 100
```

Related Commands	Command	Description
	ipv6 mld snooping filter	Filters the multicast group on the interface.

Platform N/A
Description

9.11 ipv6 mld snooping mrouter learn

Use this command to enable the switch to dynamically learn MLD query or PIM packets to identify the mrouter interface automatically.

Use the **no** form of this command to disable this function.

Use the **default** form of this command to restore the default setting.

ipv6 mld snooping [vlan *vid*] mrouter learn

no ipv6 mld snooping [vlan *vid*] mrouter learn


default ipv6 mld snooping [vlan *vid*] mrouter learn

Parameter Description	Parameter	Description
	vlan <i>vid</i>	VLAN ID, in the range from 1 to 4094

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide The routing interface is the interface of the multicast device connected with the peer device. By default, the dynamically learned routing interface is enabled on the layer-2 multicast device. Use the **no** option to disable this function and clear all dynamically-learned routing interfaces.

 With the source port check enabled, only the multicast flow through the mroute interface are valid and forwarded to the registered interface on the layer-2 multicast device. Those multicast flow through the non-mroute interface are invalid and will be discarded.

Configuration Examples The following example enables the dynamic multicast routing port learning function for VLAN1.

```
Ruijie(config)# no ipv6 mld snooping mrouter learn
Ruijie(config)# ipv6 mld snooping vlan 1 mrouter learn
```

Related Commands N/A

9.12 ipv6 mld snooping query-max-response-time

Use this command to set the maximum response time of the MLD general query packet.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

default ipv6 mld snooping query-max-response-time

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the maximum response time of the MLD general query packet in the range from 1 to 65,535 in the unit of seconds.

Defaults The default is 10 seconds.

Command Mode Interface configuration mode

Usage Guide Upon receiving the MLD general query packets, the Layer-2 multicast device updates the aging timer of all member ports. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list.

Upon receiving the MLD specific group query packets, the Layer-2 multicast device enables the aging timer of all member ports in this specific group. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list.

For the source query packets of the MLD specific group, the timer is not updated.

The configured maximum response time is effective after another query packet is received.

Configuration Examples The following example sets the maximum response time of the MLD general query packet to 100 seconds.

```
Ruijie(config)# ipv6 mld snooping query-max-response-time 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.13 ipv6 mld snooping source-check port

Use this command to enable the MLD source-check port.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping source-check port

no ipv6 mld snooping source-check port

default ipv6 mld snooping source-check port

Parameter Description	Parameter	Description
		N/A

Defaults The source-check port is disabled by default.

Command Mode Global configuration mode

Usage Guide The MLD Snooping source port check function is to limit the MLD multicast flow through the interface strictly. With the source port check disabled, all video flow are illegal and forwarded to the registered member port according to the MLD Snooping forwarding list. With the MLD Snooping source port check enabled, only the multicast flow through the mroute interface is legal and forwarded to the registered interface by the layer-2 multicast device; and the multicast flow through the non-mroute interface are illegal and discarded.

This command is used to enable the source port check globally. Once this function is enabled, all multicast flow must come from the mroute interface, or they'll be discarded.

Configuration Examples The following example enables MLD Snooping source-check port.

```
Ruijie(config)# ipv6 mld snooping source-check port
```

Related Commands	Command	Description
		N/A

Platform Description N/A

9.14 ipv6 mld snooping suppression enable

Use this command to enable the MLD Snooping suppression.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping suppression enable

no ipv6 mld snooping suppression enable

default ipv6 mld snooping suppression enable

Parameter Description	Parameter	Description
		N/A

Defaults The MLD Snooping suppression function is disabled by default.

Command Global configuration mode.
Mode

Usage Guide With the IPv6 MLD Snooping suppression function enabled, within the query interval, the layer-2 device will only forward the first received MLD Report packet in an IPv6 multicast group to the layer-3 device, but not the other MLD Report packets in the same IPv6 multicast group, reducing the packet number in the network.
This command is used to enable the IPv6 MLD Snooping suppression, and only the MLDv1 Report packets are suppressed rather than the MLDv2 Report packets.

Configuration The following example enables MLD Snooping suppression.

Examples Ruijie(config)# ipv6 mld snooping suppression enable

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

9.15 ipv6 mld snooping svgl profile

Use this command to specify the group address range to be in the SVGL mode.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping svgl profile *profile-number*

no ipv6 mld snooping svgl profile

default ipv6 mld snooping svgl profile

**Parameter
Description**

Parameter	Description
<i>profile-number</i>	Sets the profile number, in the range from 1 to 1024.

Defaults No profiles are associated with SVGL by default.

Command Global configuration mode
Mode

Usage Guide With the SVGL mode or IVGL-SVGL mode configured for the MLD Snooping working mode, a profile shall be associated with the IVGL for the purpose of specifying the group address range in the SVGL mode. That is to say, the member port of the multicast forwarding entry can be forwarded across the VLANs, while the member ports of the corresponding multicast forwarding entries within other multicast address range must belong to the same VLAN. By default, no profile is associated, which means that apply no multicast group in the SVGL mode.

Configuration The following example specifies the SVGL mode application range as the profile 2 group address range.

Examples

```
Ruijie(config)# ipv6 mld snooping svgl profile 2
```

Related Commands

Command	Description
ipv6 mld snooping ivgl	Enables the MLD Snooping and set the ivgl mode.
ipv6 mld snooping ivgl-svgl	Enables the MLD Snooping and set the ivgl-svgl mode.

Platform N/A

Description

9.16 ipv6 mld snooping svgl vlan

Use this command to specify the shared VLAN in MLD Snooping SVGL mode.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping svgl vlan *vid*

no ipv6 mld snooping svgl vlan

default ipv6 mld snooping svgl vlan

Parameter Description

Parameter	Description
<i>vid</i>	The VLAN ID, in the range from 1 to 4094.

Defaults The default is 1.

Command Global configuration mode

Mode

Usage Guide This command is used to specify the SVGL shared VLAN if MLD Snooping is running in SVGL or IVGL-SVGL mode.

Configuration The following example sets the shared VLAN in MLD Snooping SVGL mode to 5.

Examples

```
Ruijie(config)# ipv6 mld snooping svgl vlan 5
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

9.17 ipv6 mld snooping vlan

Use this command to enable the MLD Snooping function for the specified VLAN.

Use the **no** form of this command to disable this function.

Use the **default** form of this command to restore the default setting.

ipv6 mld snooping vlan *vid*

no ipv6 mld snooping vlan *vid*

default ipv6 mld snooping vlan *vid*

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID, in the range from 1 to 4094.

Defaults The MLD Snooping function is enabled by default.

Command Global configuration mode

Mode

Usage Guide By default, the MLD Snooping is enabled in all VLANs. You can disable the MLD Snooping for the specified VLAN.

Configuration The following example disables the MLD Snooping function in VLAN 2 in IVGL mode.

Examples

```
Ruijie(config)# ipv6 mld snooping ivgl
Ruijie(config)# no ipv6 mld snooping vlan 2
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

9.18 ipv6 mld snooping vlan mrouter interface

Use this command to set the static mrouter interface.

Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

no ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

default ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID, in the range from 1 to 4094.

<i>interface-type</i> <i>interface-number</i>	The interface number
--	----------------------

Defaults No static mrouter interface is configured by default.

Command Global configuration mode

Mode

Usage Guide Use this command to set the static mrouter interface for the purpose that all IPv6 multicast data received on the switch can be forwarded. With the source port check function enabled, only the multicast flow through the mroute interface can be forwarded.

Configuration The following example sets a multicast routing port.

Examples Ruijie(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitEthernet 0/1

Related Commands	Command	Description
	ipv6 mld snooping source-check port	Sets the multicast source port check.

Platform N/A

Description

9.19 ipv6 mld snooping vlan static interface

Use this command to set a static member port to receive the multicast flow for the purpose of preventing the port from being influenced by the MLD Report packets with the MLD Snooping enabled.

Uses the **no** form of this command to restore the default setting.

ipv6 mld snooping vlan vid static group-address interface interface-type interface-number

no ipv6 mld snooping vlan vid static group-address interface interface-type interface-number

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID, in the range from 1 to 4094. The default is 1.
<i>group-address</i>	The multicast address	
<i>interface-type</i> <i>interface-number</i>	The interface number	

Defaults No static member port is configured by default.

Command Global configuration mode

Mode

Usage Guide Use this command to set the interface as the member port of multiple static multicast addresses.

Configuration The following example sets the interface gigabitEthernet 0/1 as the static member port of the FF88::1 group.

Examples

```
Ruijie(config)# ipv6 mld snooping vlan 1 static FF88::1 interface
gigabitEthernet 0/1
```

**Related
Commands**

Command	Description
ipv6 mld snooping vlan mrouter interface	Sets the mrouter interface.

Platform

N/A

Description

9.20 permit

Use this command to allow the multicast flow profile within the specified range in the profile configuration mode.

permit**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

The default profile action is **deny**.

**Command
Mode**

Profile configuration mode

Usage Guide

Before configuring this command, use the range command to set the multicast range first.

**Configuration
Examples**

The following example allows the multicast flow profile within the range from FF15::1 to FF15::100 to be forwarded only.

```
Ruijie(config)# ipv6 mld snooping profile 1
Ruijie(config-profile)# range FF15::1 FF15::100
Ruijie(config-profile)# permit
```

**Related
Commands**

Command	Description
ipv6 mld profile	Creates one profile.
range	Sets the multicast address range.
deny	Sets the profile action deny.

Platform

N/A

Description

9.21 range

Use this command to specify the profile multicast flow range, which can be one single multicast address, or can be the multicast address within the specified range when configuring a profile in the profile configuration mode.

range *low-ipv6-address* [*high-ip-address*]

Parameter Description	Parameter	Description
	<i>low-ipv6-address</i>	The low address within the specified range
	<i>high-ip-address</i>	The high address within the specified range

Defaults No range is defined by default.

Command Mode Profile configuration mode

Usage Guide The value of *low-ipv6-address* shall be smaller than the one of *high-ipv6-address*. With the address range configured, an action shall be specified, and the default profile action is deny.

Configuration Examples The following example creates the multicast flow profile within the range from FF15::1 to FF15::100.

```
Ruijie(config)# ipv6 mld snooping profile 1
Ruijie(config-profile)# range FF15::1 FF15::100
Ruijie(config-profile)# permit
```

Related Commands	Command	Description
	ipv6 mld profile	Creates one profile.
	deny	Sets the profile action deny.
	permit	Sets the profile action permit.

Platform N/A

Description

9.22 show ipv6 mld profile

Use this command to display the related MLD profile configuration.

show ipv6 mld profile *profile-number*

Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number in the range from 1 to 1024

- Defaults** N/A
- Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode
- Usage Guide** Use this command to display the related MLD profile configuration.
- Configuration** The following example displays the MLD profile configuration.

Examples

```
Ruijie# show ipv6 mld profile
ipv6 mld profile    1
  permit
  range FF15::1 FF15::100

ipv6 mld profile    2
  deny
  range FF88::1 FF88::100
```

Related Commands

Command	Description
N/A	N/A

- Platform** N/A
- Description**

9.23 show ipv6 mld snooping

Use this command to display the related MLD Snooping information.

show ipv6 mld snooping [**gda-table** | **interfaces** *interface-type interface-number* | **mrouter** | **statistics** [**vlan** *vid*] | **vlan** *vid*]

Parameter Description

Parameter	Description
gda-table	Displays the multicast forwarding rule table.
Interfaces <i>interface-type interface-number</i>	Displays the MLD Snooping filtering configuration.
mrouter	Displays the information about mrouter interface.
statistics	Displays the MLD Snooping statistics.
vlan <i>vlan-id</i>	Displays the MLD Snooping information of the specified vlan.

- Defaults** N/A
- Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the related MLD Snooping information.

Configuration The following example displays the MLD Snooping configurations.

Examples

```
In IVGL mode:
Ruijie#show ipv6 mld snooping
MLD-snooping mode: IVGL
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300 (Seconds)
Dynamic Host Aging Time: 260 (Seconds)

vlan 1
-----
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC

In SVGL mode:
Ruijie#show ipv6 mld snooping
MLD-snooping mode: SVGL
SVGL vlan: 1
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300 (Seconds)
Dynamic Host Aging Time: 260 (Seconds)

In IVGL-SVGL mode:
Ruijie#show ipv6 mld snooping
MLD-snooping mode: IVGL-SVGL
SVGL vlan: 1
SVGL profile number: 1
Source port check: Disable
MLD Fast-Leave: Disable
MLD Report suppress: Disable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time: 300 (Seconds)
Dynamic Host Aging Time: 260 (Seconds)
```

```
vlan 1
-----
MLD Snooping state: Enabled
Multicast router learning mode: Enable
MLD Fast-Leave: Enabled
MLD VLAN Mode: STATIC
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A



Security Commands

- 1 AAA Commands
- 2 RADIUS Commands
- 3 TACACS+ Commands
- 4 802.1X Commands
- 5 Web Authentication Commands
- 6 SCC Commands
- 7 Global IP-MAC Binding Commands
- 8 Password-Policy Commands
- 9 Port Security Commands
- 10 Storm Control Commands
- 11 SSH Commands
- 12 URPF Commands
- 13 CPU Protection Commands
- 14 DHCP Snooping Commands
- 15 ARP-Check Commands
- 16 DAI Commands

17 IP Source Guard Commands

18 NFPP Commands

19 DoS Protection Commands

1 AAA Commands

1.1 aaa accounting commands

Use this command to configure NAS command accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting commands *level* { **default** | *list-name* } **start-stop** *method1* [*method2...*]

no aaa accounting commands *level* { **default** | *list-name* }

Parameter	Parameter	Description
Description	<i>level</i>	The accounting command level, 0-15. The message shall be recorded before which command level is executed is determined.
	default	When this parameter is used, the following defined method list is used as the default method for command accounting.
	<i>list-name</i>	Name of the command accounting method list, which could be any character strings.
	<i>method</i>	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
	none	Does not perform accounting.
	group	Uses the server group for accounting, the TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service. The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration The following example enables NAS command accounting.

Examples

```
Ruijie(config)# aaa accounting commands 15 default start-stop group tacacs+
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authentication	Defines AAA authentication.
	accounting commands	Applies the accounting commands to the terminal line.

Platform N/A

Description

1.2 aaa accounting exec

Use this command to enable NAS access accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting exec { **default** | *list-name* } **start-stop** *method1* [*method2...*]

no aaa accounting exec { **default** | *list-name* }

Parameter	Parameter	Description
Description	default	When this parameter is used, the following defined method list is used as the default method for Exec accounting.
	<i>list-name</i>	Name of the Exec accounting method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: none and group . One method list can contain up to four methods.
	none	Does not perform accounting.
	group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide RGOS enables the exec accounting function after enabling the login authentication. After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user logs in, it does not send the account stop information to the security server when a user logs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration The following example enables NAS access accounting.

Examples

```
Ruijie(config)# aaa accounting network start-stop group radius
```

Related	Command	Description
Commands	aaa new-model	Enables the AAA security service.
	aaa authentication	Defines AAA authentication.
	accounting commands	Applies the Exec accounting to the terminal line.

Platform N/A
Description

1.3 aaa accounting network

Use this command to enable network access accounting.
 Use the **no** form of this command to restore the default setting.
aaa accounting network { default | list-name } start-stop method1 [method2..]
no aaa accounting network { default | list-name }

Parameter	Parameter	Description
Description	default	When this parameter is used, the following defined method list is used as the default method for Network accounting.
	<i>list-name</i>	Name of the accounting method list
	<i>method</i>	Sends accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
	none	Does not perform accounting.
	group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS performs accounting of user activities by sending record attributes to the security server. Use the **start-stop** keyword to set the user accounting option.

Configuration Examples The following example enables network access accounting.

```
Ruijie(config)# aaa accounting network start-stop group radius
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization network	Defines a network authorization method list.
	aaa authentication	Defines AAA authentication.
	username	Defines a local user database.

Platform N/A
Description

1.4 aaa accounting update

Use this command to enable the accounting update function.

Use the **no** form of this command to restore the default setting.

aaa accounting update

no aaa accounting update

Parameter

N/A

Description

Defaults

This function is disabled by default.

Command

Global configuration mode

Mode

Usage Guide

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration

The following example enables the accounting update function.

Examples

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
```

Related

Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform

N/A

Description

1.5 aaa accounting update periodic

Use this command to set the interval of sending the accounting update message.

Use the **no** form of this command to restore the default setting.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter

Parameter

Description

Description

interval

Interval of sending the accounting update message, in the unit of minutes. The shortest interval is 1 minute.

Defaults

The default is 5 minutes.

Command

Global configuration mode

Mode

Usage Guide If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration The following example sets the interval of accounting update to 1 minute.

Examples

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
Ruijie(config)# aaa accounting update periodic 1
```

Related**Commands**

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform N/A

Description

1.6 aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list.

Use the **no** form of this command to delete the 802.1x user authentication method list.

aaa authentication dot1x { **default** | *list-name* } *method1* [*method2...*]

no aaa authentication dot1x { **default** | *list-name* }

Parameter**Description**

Parameter	Description
default	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.
<i>list-name</i>	Name of the 802.1x user authentication method list, which could be any character string
<i>method</i>	It must be one of the keywords: local , none and group . One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.

Defaults N/A

Command Global configuration mode

Mode

Usage Guide If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use the **aaa authentication dot1x** command to configure a default or optional method list for 802.1x user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples The following example defines an AAA authentication method list named **RDS_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication dot1x rds_d1x group radius local
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	dot1x authentication	Associates a specific method list with the 802.1x user.
	username	Defines a local user database.

Platform N/A

Description

1.7 aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list.

Use the **no** form of this command to delete the user authentication method list.

aaa authentication enable default *method1* [*method2...*]

no aaa authentication enable default

Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
	<i>method</i>	It must be one of the keywords: local , none and group . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
	enable	Enables AAA Enable authentication.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable

authentication negotiation. You must use the **aaa authentication enable** command to configure a default or optional method list for Enable authentication.

The next method can be used for authentication only when the current method does not work.

The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

Configuration Examples The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication enable default group radius local
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	enable	Switchover the user level.
	username	Defines a local user database.

Platform N/A
Description

1.8 aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication login { **default** | *list-name* } *method1* [*method2..*]

no aaa authentication login { **default** | *list-name* }

Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
	<i>list-name</i>	Name of the user authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: local , none , group and subs . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
	subs	Uses the subs database for authentication.

Defaults N/A

Command Global configuration mode

Mode

Usage Guide If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use the **aaa authentication login** command to configure a default or optional method list for Login authentication.

The next method can be used for authentication only when the current method does not work.

You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

Configuration Examples The following example defines an AAA Login authentication method list named list-1. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication login list-1 group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
login authentication	Applies the Login authentication method to the terminal lines.
username	Defines a local user database.

Platform N/A

Description

1.9 aaa authentication ppp

Use this command to enable the AAA authentication for PPP user and configure the PPP user authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication ppp { **default** | *list-name* } *method1* [*method2...*]

no aaa authentication ppp { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.
<i>list-name</i>	Name of the user authentication method list, which could be any character strings
<i>method</i>	It must be one of the keywords: local , none group and subs . One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the AAA PPP security service is enabled on the device, users must use AAA authentication for PPP negotiation. You must use the **aaa authentication ppp** command to configure a default or optional method list for PPP user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples The following example defines an AAA authentication method list named rds_ppp for PPP session. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication ppp rds_ppp group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
ppp authentication	Associates a specific method list with the PPP user.
username	Defines a local user database.

Platform Description N/A

1.10 aaa authentication sslvpn

Use this command to enable AAA authentication for the SSL VPN user and configure the SSL VPN user authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication sslvpn { default | list-name } method1 [method2...]

no aaa authentication sslvpn { default | list-name }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for SSL VPN user authentication.
<i>list-name</i>	Name of SSL VPN user authentication method list, which could be any character strings
<i>method</i>	It must be one of the keywords: local , none , subs and group . One method list can contain up to four methods.
local	Use the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS

	server group is supported.
subs	Uses the subs database for authentication.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the SSL VPN security service is enabled on the device, users must use the AAA authentication for SSL VPN negotiation. You must use the **aaa authentication sslvpn** command to configure a default or optional method list for user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples The following example defines an AAA authentication method list named **rds_sslvpn** for SSL VPN session. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication sslvpn rds_sslvpn group radius local
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.11 aaa authentication web-auth

Use this command to enable AAA second-generation Web authentication and configure the second-generation Web authentication method list in global configuration mode.

Use the **no** form of this command to delete the authentication method list.

aaa authentication web-auth { **default** | *list-name* } *method1* [*method2...*]

no aaa authentication web-auth { **default** | *list-name* }

Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for the second-generation Web authentication.
	<i>list-name</i>	Name of second-generation Web authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: local , none , subs and group . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS

	server group is supported.
subs	Uses the subs database for authentication.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the AAA second-generation Web security service is enabled on the device, users must use AAA for the second-generation Web authentication negotiation. You must use the **aaa authentication web-auth** command to configure a default or optional method list for user authentication. The next method can be used for authentication only when the current method does not work.

Configuration Examples The following example defines an AAA authentication method list named **rds_web**. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication web-auth rds_web group radius none
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.12 aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI. Use the **no** form of this command to restore the default setting.

aaa authorization commands *level* { **default** | *list-name* } *method1* [*method2...*]

no aaa authorization commands *level* { **default** | *list-name* }

Parameter Description	Parameter	Description
	<i>level</i>	Command level to be authorized in the range from 0 to 15
	default	When this parameter is used, the following defined method list is used as the default method for command authorization.
	<i>list-name</i>	Name of the user authorization method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: none and group . One method list can contain up to four methods.
	none	Do not perform authorization.
	group	Uses the server group for authorization. At present, the TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny.

It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.

The configured command authorization method must be applied to terminal line which requires the command authorization. Otherwise, the configured command authorization method is ineffective.

Configuration The following example uses the TACACS+ server to authorize the level 15 command.

Examples Ruijie(config)# aaa authorization commands 15 default group tacacs+

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	authorization commands	Applies the command authorization for the terminal line.

Platform N/A

Description

1.13 aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode).

Use the **no** form of this command to restore the default setting.

aaa authorization config-commands

no aaa authorization config-commands

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.

Configuration The following example enables the configuration command authorization function.

Examples

```
Ruijie(config)# aaa authorization config-commands
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization commands	Defines the AAA command authorization.

Platform N/A

Description

1.14 aaa authorization console

Use this command to authorize the commands of the users who have logged in the console.

Use the **no** form of this command to restore the default setting.

aaa authorization console

no aaa authorization console

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide RGOS supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.

Configuration The following example enables the aaa authorization console function.

Examples

```
Ruijie(config)# aaa authorization console
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization commands	Defines the AAA command authorization.
	authorization commands	Applies the command authorization to the terminal line.

Platform N/A

Description

1.15 aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level.

Use the **no** form of this command to restore the default setting.

aaa authorization exec { **default** | *list-name* } *method1* [*method2...*]

no aaa authorization exec { **default** | *list-name* }

Parameter	Parameter	Description
Description	default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
	<i>list-name</i>	Name of the user authorization method list, which could be any character strings
	<i>method</i>	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
	local	Uses the local user name database for authorization.
	none	Does not perform authorization.
	group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide RGOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The **aaa authorization exec** function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the **aaa authorization exec**. You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

Configuration The following example uses the RADIUS server to authorize Exec.

Examples

```
Ruijie(config)# aaa authorization exec default group radius
```

Related	Command	Description
Commands	aaa new-model	Enables the AAA security service.
	authorization exec	Applies the command authorization to the terminal line.
	username	Defines a local user database.

Platform N/A

Description

1.16 aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network.

Use the **no** form of this command to restore the default setting.

aaa authorization network { **default** | *list-name* } *method1* [*method2...*]

no aaa authorization network { **default** | *list-name* }

Parameter	Parameter	Description
Description	default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
	<i>method</i>	It must be one of the keywords: none and group. One method list can contain up to four methods.
	none	Does not perform authorization.
	group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.

Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.

The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

Configuration Examples The following example uses the RADIUS server to authorize network services.

```
Ruijie(config)# aaa authorization network default group radius
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa accounting	Defines AAA accounting.
	aaa authentication	Defines AAA authentication.
	username	Defines a local user database.

Platform Description N/A

1.17 aaa domain

Use this command to configure the domain attributes.

Use the **no** form of this command to restore the default setting.

aaa domain { **default** | *domain-name* }

no aaa domain { **default** | *domain-name* }

Parameter	Parameter	Description
Description	default	Uses this parameter to configure the default domain.
	<i>domain-name</i>	The name of the specified domain

Defaults No domain is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the domain-name-based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this *domain name*, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

Configuration The following example configures the domain name.

Examples

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)#
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform N/A

Description

1.18 aaa domain enable

Use this command to enable domain-name-based AAA service.

Use the **no** form of this command to restore the default setting.

aaa domain enable

no aaa domain enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide To perform the domain-name-based AAA service configuration, enable this service.

Configuration The following example enables the domain-name-based AAA service.

Examples

```
Ruijie(config)# aaa domain enable
```

Related	Command	Description
Commands	aaa new-model	Enables the AAA security service.
	show aaa doamain	Displays the domain configuration.

Platform N/A

Description

1.19 aaa local authentication attempts

Use this command to set login attempt times.

aaa local authentication attempts *max-attempts*

Parameter	Parameter	Description
Description	<i>max-attempts</i>	In the range from 1 to 2,147,483,647

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide Use this command to configure login attempt times.

Configuration The following example sets login attempt times to 6.

Examples

```
Ruijie #configure terminal
Ruijie(config)#aaa local authentication attempts 6
```

Related	Command	Description
Commands	show running-config	Displays the current configuration of the switch.
	show aaa lockout	Displays the lockout configuration parameter of current login.

Platform N/A

Description

1.20 aaa local authentication lockout-time

Use this command to configure the lockout-time period when the login user has attempted for more than the limited times.

aaa local authentication lockout-time *lockout-time*

Parameter	Parameter	Description
Description	<i>lockout-time</i>	In the range from 1 to 2,147,483,647 in the unit of minutes

Defaults The default is 15 minutes.

Command Mode Global configuration mode

Usage Guide Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.

Configuration Examples The following example sets the lockout-time period to 5 minutes.

```
Ruijie#configure terminal
Ruijie(config)#aaa local authentication lockout-time 5
```

Related Commands	Command	Description
	show running-config	Displays the current configuration of the switch.
	show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description N/A

1.21 aaa log enable

Use this command to enable the system to print the syslog informing AAA authentication success. Use the **no** form of this command to restore the default setting.

aaa log enable

no aaa log enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the system to print the syslog informing aaa authentication success.

Configuration The following example disables the system to print the syslog informing aaa authentication success.

Examples

```
Ruijie(config)# no aaa log enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.22 aaa new-model

Use this command to enable the RGOS AAA security service.

Use the **no** form of this command to restore the default setting.

aaa new-model

no aaa new-model

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

Configuration The following example enables the AAA security service.

Examples

```
Ruijie(config)# aaa new-model
```

Related Commands	Command	Description
	aaa authentication	Defines a user authentication method list.
	aaa authorization	Defines a user authorization method list.
	aaa accounting	Defines a user accounting method list.

Platform N/A

Description

1.23 access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the

IEEE802.1 users.

Use the **no** form of this command to restore the default setting.

access-limit *num*

no access-limit

Parameter	Parameter	Description
Description	<i>num</i>	The number used for the user limitation is only valid for the IEEE802.1 users.

Defaults By default, no number of users is limited.

Command Domain configuration mode

Mode

Usage Guide This command limits the number of users for the domain.

Configuration The following example sets the number of users to 20 for the domain named ruijie.com.

Examples

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# access-limit 2
```

Related	Command	Description
Commands	aaa new-model	Enables the AAA security service.
	aaa domain enable	Switchover the user level.
	show aaa domain	Defines a local user database.

Platform N/A

Description

1.24 accounting network

Use this command to configure the Network accounting list.

Use the **no** form of this command to restore the default setting.

accounting network { **default** | *list-name* }

no accounting network

Parameter	Parameter	Description
Description	default	Uses this parameter to specify the default method list.
	<i>list-name</i>	The name of the network accounting list

Defaults With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.

Command Domain configuration mode

Mode

Usage Guide Use this command to configure the Network accounting method list for the specified domain.

Configuration The following example sets the Network accounting method list for the specified domain.

Examples

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# accounting network default
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform N/A

Description

1.25 authentication dot1x

Use this command to configure the IEEE802.1x authentication list.

Use the **no** form of this command to restore the default setting.

authentication dot1x { **default** | *list-name* }

no authentication dot1x

Parameter	Parameter	Description
Description	default	Uses this parameter to specify the default method list
	<i>list-name</i>	The name of the specified method list

Defaults With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command Domain configuration mode

Mode

Usage Guide Specify an IEEE802.1x authentication method list for the domain.

Configuration The following example sets an IEEE802.1x authentication method list for the specified domain.

Examples

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# authentication dot1x default
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform N/A

Description

1.26 authorization network

Use this command to configure the Network authorization list.

Use the **no** form of this command to restore the default setting.

authorization network { **default** | *list-name* }

no authorization network

Parameter	Parameter	Description
Description	default	Uses this parameter to specify the default method list.
	<i>list-name</i>	The name of the specified method list

Defaults With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command Mode Domain configuration mode

Usage Guide Specify an authorization method list for the domain.

Configuration The following example sets an authorization method list for the specified domain.

Examples

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# authorization network default
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform N/A

Description

1.27 clear aaa local user lockout

Use this command to clear the lockout user list.

clear aaa local user lockout { **all** | *user-name word* }

Parameter	Parameter	Description
Description	all	Indicates all locked users.
	<i>user-name word</i>	Indicates the ID of the locked User.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear all the user lists or a specified user list.

Configuration The following example clears the lockout user list.

Examples

```
Ruijie(config)# clear aaa local user lockout all
```

Related Commands	Command	Description
	show running-config	Displays the current configuration of the switch.
	show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description N/A

1.28 show aaa accounting update

Use this command to display the accounting update information.

show aaa accounting update

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the accounting update interval and whether the accounting update is enabled.

Configuration The following example displays the accounting update information.

Examples

```
Ruijie# show aaa accounting update
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.

Platform Description N/A

1.29 show aaa domain

Use this command to display all current domain information.

show aaa domain [**default** | *domain-name*]

Parameter	Parameter	Description
Description	default	Displays the default domain.
	<i>domain-name</i>	Displays the specified domain.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide If no domain-name is specified, all domain information will be displayed.

Configuration The following example displays the domain named domain.com.

Examples

```
Ruijie(config)# show aaa domain domain.com
=====Domain domain.com=====
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.

Platform N/A

Description

1.30 group

Use this command to display all the server groups configured for AAA.

show aaa group

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following command displays all the server groups.

Examples

```
Ruijie# show aaa group
Type      Reference Name
-----
radius    1      radius
tacacs+   1      tacacs+
radius    1      dot1x_group
radius    1      login_group
radius    1      enable_group
```

Related Commands	Command	Description
	aaa group server	Configures the AAA server group.

Platform N/A

Description

1.31 show aaa lockout

Use this command to display the lockout configuration.

show aaa lockout

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the lockout configuration.

Configuration The following example displays the lockout configuration.

Examples

```
Ruijie# show aaa lockout
Lock tries:    3
Lock timeout: 15 minutes
```

Related	Command	Description
---------	---------	-------------

Commands	N/A	N/A
-----------------	-----	-----

Platform N/A

Description

1.32 show aaa method-list

Use this command to display all AAA method lists.

show aaa method-list

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Mode

Usage Guide Use this command to display all AAA method lists.

Configuration The following example displays the AAA method list.

Examples

```
Ruijie# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local group angel group rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorization network default group radius
```

Related	Command	Description
Commands	aaa authentication	Defines a user authentication method list
	aaa authorization	Defines a user authorization method list
	aaa accounting	Defines a user accounting method list

Platform N/A

Description

1.33 show aaa user

Use this command to display AAA user information.

show aaa user { all | lockout | by-id *session-id* | by-name *user-name* }

Parameter	Parameter	Description
Description	all	Displays all AAA user information.
	lockout	Displays the locked AAA user information.
	by-id <i>session-id</i>	Displays the information of the AAA user that with a specified session ID.
	by-name <i>user-name</i>	Displays the information of the AAA user with a specified user name.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display AAA user information.

Configuration Examples The following example displays AAA user information.

```
Ruijie#show aaa user all
-----
      Id ----- Name
2345687901      wwxy
-----

Ruijie# show aaa user by-id 2345687901
-----
      Id ----- Name
2345687901      wwxy

Ruijie# show aaa user by-name wwxy
-----
      Id ----- Name
2345687901      wwxy
-----

Ruijie# show aaa user lockout
```

Name	Tries	Lock	Timeout (min)

Ruijie#			

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

1.34 state

Use this command to set whether the configured domain is valid.

Use the **no** form of this command to restore the default setting.

state { block | active }

no state

Parameter	Parameter	Description
Description	block	The configured domain is invalid.
	active	The configured domain is valid.

Defaults The default is active.

Command Mode Domain configuration mode

Usage Guide Use this command to set whether the specified configured domain is valid.

Configuration Examples The following example sets the configured domain to be invalid.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# state block
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain enable	Displays the domain configuration.

Platform N/A
Description

1.35 username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Use the **no** form of this command to restore the default setting.

username-format { **without-domain** | **with-domain** }

no username-format

Parameter	Parameter	Description
Description	without-domain	Sets the user name without the domain information.
	with-domain	Sets the user name with the domain information.

Defaults The default is without-domain.

Command Domain configuration mode

Mode

Usage Guide Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Configuration The following example sets the user name without the domain information.

Examples

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# username-domain without-domain
```

Related	Command	Description
Commands	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform N/A

Description

2 RADIUS Commands

2.1 aaa group server radius

Use this command to enter AAA server group configuration mode.

Use the **no** form of this command to restore the default setting.

aaa group server radius *name*

no aaa group server radius *name*

Parameter Description	Parameter	Description
	<i>name</i>	Server group name. Keywords "radius" and "tacacs +" are excluded as they are the default RADIUS and TACACS+ server group names.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure a RADIUS AAA server group.

Configuration Examples The following example configures a RADIUS AAA server group named ss.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type      Reference Name
-----
radius    1          radius
tacacs+   1          tacacs+
radius    1          ss
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.2 ip oob

Use this command to specify the MGMT port used in the TACACS+ server group.

Use the **no** form of this command to restore the default setting.

ip oob [*via mgmt_name*]

no ip oob

Parameter	Parameter	Description
Description	<i>mgmt_name</i>	MGMT port name

Defaults N/A

Command Mode TACACS+ server group configuration mode

Usage Guide Use the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode. If no port is specified as the MGMT port. MGMT Port 0 is default.

Configuration The following example specifies MGMT port 1 used in the TACACS+ server group.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.14
Ruijie(config-gs-radius)# server 192.168.4.15
Ruijie(config-gs-radius)# ip oob via mgmt 1
Ruijie(config-gs-radius)# end
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.3 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packet.

Use the **no** form of this command to delete the source IP address for the RADIUS packet.

ip radius source-interface *interface-name*

no radius source-interface *interface-name*

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface that the source IP address of the RADIUS packet belongs to.

Defaults The source IP address of the RADIUS packet is set by the network layer.

Command Global configuration mode
mode

Usage Guide In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

Configuration Examples The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface and uses it as the source IP address of the RADIUS packet.

```
Ruijie(config)# ip radius source-interface fastEthernet 0/0
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS server.
ip address	Configures the IP address of the interface.

Platform N/A
Description

2.4 ip vrf forwarding

Use this command to select a VRF for the AAA server group.

Use the **no** form of this command to restore the default setting.

ip vrf forwarding *vrf_name*

no ip vrf forwarding

Parameter Description

Parameter	Description
<i>vrf_name</i>	VRF name

Defaults N/A

Command Mode Server group configuration mode

Usage Guide This command is used to select a VRF for the specified server.

Configuration Examples The following example selects the VRF named *vrf_name* for AAA server group *ss*.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.12
Ruijie(config-gs-radius)# server 192.168.4.13
Ruijie(config-gs-radius)# ip vrf forwarding vrf_name
Ruijie(config-gs-radius)# end
```


Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.5 radius set qos cos

Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface. Use the **no** form of this command to restore the default setting.

radius set qos cos

no radius set qos cos

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Set the QoS value sent by the RADIUS server as the DSCP value.

Command Mode Global configuration mode.

Usage Guide This command is used to set the QoS value sent by the RADIUS server as the CoS value, and the DSCP value by default.

Configuration Examples The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface:

```
Ruijie(config)# radius set qos cos
```

Related Commands	Command	Description
	radius vendor-specific extend	Extends RADIUS as not to differentiate the IDs of private vendors.

Platform N/A
Description

2.6 radius support cui

Use this command to enable RADIUS to support the cui function.

Use the **no** form of this command to restore the default setting.

radius support cui

no radius support cui

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable RADIUS to support the cui function.

Configuration Examples The following example enables RADIUS to support the cui function.

```
Ruijie(config)# radius support cui
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.7 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors.

Use the **no** form of this command to restore the default setting.

radius vendor-specific extend

no radius vendor-specific extend

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Only the private vendor IDs of Ruijie are recognized.

Command Mode Global configuration mode

Usage Guide This command is used to identify the attributes of all vendor IDs by type.

Configuration The following example extends RADIUS so as not to differentiate the IDs of private vendors:

Examples `Ruijie(config)# radius vendor-specific extend`

**Related
Commands**

Command	Description
<code>radius attribute</code>	Configures vendor type.
<code>radius set qos cos</code>	Sets the QoS value sent by the RADIUS server as the cos value of the interface.

Platform N/A

Description

2.8 radius-server account update retransmit

Use this command to configure accounting update packet retransmission for the Web authentication user.

Use the **no** form of this command to restore the default setting,

radius-server account update retransmit

no radius-server account update retransmit

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide This command is used to configure accounting update packet retransmission for the Web authentication user exclusively.

Configuration Examples The following example configures accounting update packet retransmission for the Web authentication user.

```
Ruijie(config)#radius-server account update retransmit
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

2.9 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute.

Use the **no** form of this command to restore the default setting.

radius-server attribute 31 mac format { ietf | normal | unformatted }

no radius-server attribute 31 mac format

Parameter Description

Parameter	Description
ietf	The standard format specified by the IETF RFC3580. '-' is used as the separator, for example: 00-D0-F8-33-22-AC.
normal	Normal format representing the MAC address. '.' is used as the separator. For example: 00d0.f833.22ac.
unformatted	No format and separator. By default, unformatted is used. For example: 00d0f83322ac.

Defaults The default format is unformatted.

Command Mode Global configuration mode

Usage Guide Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

Configuration Examples The following example defines the RADIUS Calling-Station-ID attribute as IETF format.

```
Ruijie(config)# radius-server attribute 31 mac format ietf
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS server.

Platform Description N/A

2.10 radius-server dead-criteria

Use this command to configure criteria on a device to determine that the Radius server is unreachable.

Use the **no** form of this command to restore the default setting.

radius-server dead-criteria { time seconds [tries number] | tries number }

no radius-server dead-criteria { time seconds [tries number] | tries number }

Parameter

Parameter	Description
-----------	-------------

Description	
time <i>seconds</i>	Configures the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds.
tries <i>number</i>	Configures the successive timeout times. When sending a request from the device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range from 1 to 100 in the unit of seconds.

Defaults The default **time** *seconds* is 60 and **tries** *number* is 10.

Command Mode Global configuration mode

Usage Guide If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

Configuration The following example sets the timeout to 120 seconds and timeout times to 20.

Examples Ruijie(config)# radius-server dead-criteria time 120 tries 20

Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable Radius server.
	radius-server timeout	Defines the timeout for the packet re-transmission.

Platform N/A

Description

2.11 radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable Radius server.

Use the **no** form of this command to restore the default setting.

radius-server deadtime *minutes*

no radius-server deadtime

Parameter Description	Parameter	Description

<i>minutes</i>	Defines the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range from 1 to 1,440 in the unit of minutes.
----------------	--

Defaults The default value of minutes is 0, that is, the device keeps sending requests to the unreachable Radius server.

Command Mode Global configuration mode

Usage Guide If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorter than the unreachable time.

Configuration The following example sets the duration when the device stops sending requests to 1 minute.

Examples Ruijie(config)# radius-server deadtime 1

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server dead-criteria	Defines the criteria to determine that a Radius server is unreachable.

Platform Description N/A

2.12 radius-server host

Use this command to specify a RADIUS security server host.

Use the **no** form of this command to restore the default setting.

```
radius-server host [ oob [ via mgmt-name ] ] { ipv4-address | ipv6-address } [ auth-port
port-number ] [ acct-port port-number ] [ test username name [ idle-time time ]
[ ignore-auth-port ] [ ignore-acct-port ] ] [ key [ 0 | 7 ] text-string ]
no radius-server host { ipv4-address | ipv6-address }
```

Parameter Description

Parameter	Description
oob [via mgmt-name]	Specifies an MGMT port as the source port for TACACS+ communication. The default is MGMT Port 0.
<i>ipv4-address</i>	IPv6 address of the RADIUS security server host.
<i>ipv6-address</i>	IPv4 address of the RADIUS security server host.
<i>auth-port</i>	UDP port used for RADIUS authentication.
<i>port-number</i>	Number of the UDP port used for RADIUS authentication. If it is set to

	0, this host does not perform authentication.
<i>acct-port</i>	UDP port used for RADIUS accounting.
<i>port-number</i>	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
test username <i>name</i>	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
idle-time <i>time</i>	(Optional) Sets the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
ignore-auth-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
ignore-acct-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
key [0 7] <i>text-string</i>	Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0.

Defaults No RADIUS host is specified by default.

Command Mode Global configuration mode

Usage Guide In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

Configuration Examples The following example defines a RADIUS security server host:

```
Ruijie(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
Ruijie(config)# radius-server host 192.168.100.1 test username viven idle-time 60 ignore-acct-port
```

The following example defines a RADIUS security server host in the IPv6 environment

```
Ruijie(config)# radius-server host 3000::100
```

Related Commands

Command	Description
aaa authentication	Defines the AAA authentication method list
radius-server key	Defines a shared password for the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.

Platform N/A
Description

2.13 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server.

Use the **no** form of this command to restore the default setting.

radius-server key [0 | 7] *text-string*

no radius-server key

Parameter Description	Parameter	Description
	<i>text-string</i>	Text of the shared password
	0 7	Password encryption type. 0: no encryption; 7: Simply-encrypted.

Defaults No shared password is specified by default.

Command

Mode Global configuration mode.

Usage Guide A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

Configuration The following example defines the shared password **aaa** for the RADIUS security server:

Examples Ruijie(config)# radius-server key aaa

Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server retransmit	Defines the number of RADIUS packet retransmissions.
	radius-server timeout	Defines the timeout for the RADIUS packet.

Platform N/A
Description

2.14 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond.

Use the **no** form of this command to restore the default setting.

radius-server retransmit *retries*

no radius-server retransmit

Parameter Description	Parameter	Description
	<i>retries</i>	Number of retransmissions in the range from 1 to 100

Defaults The default is 3.

Command Mode Global configuration mode.

Usage Guide AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

Configuration The following example sets the number of retransmissions to 4.

Examples

```
Ruijie(config)# radius-server retransmit 4
```

Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server key	Defines a shared password for the RADIUS server.
	radius-server timeout	Defines the timeout for the RADIUS packet.

Platform N/A

Description

2.15 radius-server source-port

Use this command to configure the source port to send RADIUS packets.

Use the **no** form of this command to restore the default setting.

radius-server source-port *port*

no radius-server source-port

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	<i>port</i>	The port ID, in the range from 0 to 65535.

Defaults The default is a random number.

Command Global configuration mode

Mode

Usage Guide The source port is random by default. This command is used to specify a source port.

Configuration The following example configures source port 10000 to send RADIUS packets.

Examples Ruijie(config)# radius-server source-port 10000

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.16 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet.

Use the **no** form of this command to restore the default setting.

radius-server timeout *seconds*

no radius-server timeout

Parameter Description	Parameter	Description
	<i>seconds</i>	Timeout in the range from 1 to 1,000 in the unit of seconds.

Defaults The default is 5 seconds.

Command

Mode Global configuration mode

Usage Guide This command is used to change the timeout of packet retransmission.

Configuration The following example sets the timeout to 10 seconds.

Examples Ruijie(config)# radius-server timeout 10

Related Commands	Command	Description

radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of the RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.

Platform N/A

Description

2.17 server auth-port acct-port

Use this command to add the server of the AAA server group.

Use the **no** form of this command to restore the default setting.

server { *ipv4-addr* | *ipv6-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

no server { *ipv4-addr* | *ipv6-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

Parameter Description	Parameter	Description
	<i>ip-addr</i>	Server IP address
	<i>ipv6-addr</i>	Server IPv6 address
	<i>port1</i>	Server authentication port
	<i>port2</i>	Server accounting port

Defaults No server is configured by default.

Command Server group configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type      Reference Name
-----
radius    1          radius
tacacs+   1          tacacs+
radius    1          ss
```

Related	Command	Description
---------	---------	-------------

Commands		
	N/A	N/A

Platform N/A

Description

2.18 show radius acct statistics

Use this command to display RADIUS accounting statistics.

show radius acct statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays RADIUS accounting statistics.

Examples

```
Ruijie#show radius acct statistics
Accounting Servers:

Server Index..... 1
Server Address..... 192.168.1.1
Server Port..... 1813
Msg Round Trip Time..... 0 (msec)
First Requests..... 1
Retry Requests..... 1
Accounting Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests.....
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.19 show radius auth statistics

Use this command to display RADIUS authentication statistics.

show radius auth statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays RADIUS authentication statistics.

Examples

```
Ruijie#show radius auth statistics
Authentication Servers:

Server Index..... 1
Server Address..... 192.168.1.1
Server Port..... 1812
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.20 show radius group

Use this command to display RADIUS server group configuration.

show radius group

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays RADIUS server group configuration.

Examples

```
Ruijie#show radius group
=====Radius group radius=====
Vrf:not-set
Server:192.168.1.1
  Server key:ruijie
  Authentication port:1812
  Accounting port:1813
  State:Active
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.21 show radius parameter

Use this command to display global RADIUS server parameters.

show radius parameter

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays global RADIUS server parameters.

Examples Ruijie# show radius parameter

```
Server Timeout: 5 Seconds
Server Deadtime: 0 Minutes
Server Retries: 3
Server Dead Criteria:
Time: 10 Seconds
Tries: 10
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.22 show radius server

Use this command to display the configuration of the RADIUS server.

show radius server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the configuration of the RADIUS server.

Examples Ruijie# show radius server

```
Server IP: 192.168.4.12
Accounting Port: 23
Authen Port: 77
Test Username: viven
```

```

Test Idle Time:  10 Minutes
Test Ports:      Authen
Server State:    Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP:       192.168.4.13
Accounting Port: 45
Authen Port:     74
Test Username:   <Not Configured>
Test Idle Time:  60 Minutes
Test Ports:      Authen and Accounting
Server State:    Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0

```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform N/A
Description

2.23 show radius vendor-specific

Use this command to display the configuration of the private vendors.

show radius vendor-specific

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the configuration of the private vendors.

```

Examples Ruijie#show radius vendor-specific
id      vendor-specific      type-value
-----
1       max-down-rate           1
2       port-priority          2
3       user-ip              3
4       vlan-id             4
5       last-supPLICANT-vers 5
        ion
6       net-ip             6
7       user-name          7
8       password           8
9       file-directory     9
10      file-count         10
11      file-name-0        11
12      file-name-1        12
13      file-name-2        13
14      file-name-3        14
15      file-name-4        15
16      max-up-rate        16
17      current-supPLICANT-version 17
18      flux-max-high32    18
19      flux-max-low32     19
20      proxy-avoid        20
21      dialup-avoid       21
22      ip-privilege       22
23      login-privilege    42
26      ipv6-multicast-adre 79
        ss
27      ipv4-multicast-adre 87
        ss
    
```

Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.

radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform N/A

Description

3 TACACS+ Commands

3.1 aaa group server tacacs+

Use this command to configure different groups of TACACS+ server hosts.

Use the **no** form of this command to remove a specified TACACS server group.

aaa group server tacacs+ group_name

no aaa group server tacacs+ group_name

Parameter Description

Parameter	Description
<i>group_name</i>	TACACS+ server group name, which cannot be radius or tacacs+ . The two names are the built-in group name.

Defaults No TACACS+ server group is configured.

**Command
Mode** Global configuration mode

Usage Guide After you group different TACACS+ servers, the tasks of authentication, authorization and accounting can be implemented by different server groups.

**Configuration
Examples** The following example configures a TACACS+ server group named tac1, and configures a TACACS+ server with IP address 1.1.1.1 in this group:

```
Ruijie(config)#aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs)# server 1.1.1.1
```

Related Commands

Command	Description
server	Configures server list of TACACS+ server group.
ip vrf forwarding	Configures VRF name supported by TACACS+ server group.

**Platform
Description** N/A

3.2 ip oob

Use this command to specify the MGMT port used in the TACACS+ server group.

Use the **no** form of this command to restore the default setting.

ip oob [via mgmt_name]

no ip oob

Parameter Description	Parameter	Description
	<i>mgmt_name</i>	MGMT port name
Defaults	N/A	
Command Mode	TACACS+ server group configuration mode	
Usage Guide	Use the aaa group server tacacs+ command to enter TACACS+ server group configuration mode. No MGMT port is specified by default.	
Configuration	The following example specifies MGMT port 1 used in the TACACS+ server group.	
Examples	<pre>Ruijie(config)# aaa group server tacacs+ ss Ruijie(config-gs-tacacs)# server 1.1.1.1 Ruijie(config-gs-tacacs)# ip oob via mgmt 1</pre>	
Platform	N/A	
Description		

3.3 ip tacacs source-interface

Use this command to use the IP address of a specified interface for all outgoing TACACS+ packets. Use the **no** form of this command to disable use of the specified interface IP address.

ip tacacs source-interface *interface-name*

no ip tacacs source-interface *interface-name*

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface for the outgoing TACACS+ packets
Defaults	The source IP address of TACACS+ packets is set on the network layer.	
Command Mode	Global configuration mode	
Usage Guide	<p>To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.</p> <p>This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer 3 devices. If the specified interface is in a VRF instance, the route of this VRF instance is used for packet transmission.</p>	

Configuration The following example specifies the IP address of GigabitEthernet 0/0 for the outgoing TACACS+ packets.

Examples

```
Ruijie(config)# ip tacacs source-interface gigabitEthernet 0/0
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ server.
ip address	Configures the IP address of an interface.

Platform N/A

Description

3.4 ip vrf forwarding

Use this command to configure the VRF used in the TACACS+ server group.

Use the **no** form of this command to remove the VRF configuration from the TACACS+ server group.

ip vrf forwarding *vrf-name*

no ip vrf forwarding

Parameter Description

Parameter	Description
<i>vrf-name</i>	VRF name

Defaults N/A

Command TACACS+ server group configuration mode

Mode

Usage Guide Before you configure this command, you need to use the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.
The VRF instance must exist and be configured with a correct VRF name through the **vrf definition** command.

Configuration The following example specifies the VRF instance named vpn1 for the TACACS+ server group:

Examples

```
Ruijie(config)# aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs)# server 1.1.1.1
Ruijie(config-gs-tacacs)# ip vrf forwarding vpn1
```

Related Commands

Command	Description
aaa group server tacacs+	Configures the TACACS+ server group.
server	Configures a server list of TACACS+ server group.

Platform N/A

Description

3.5 server

Use this command to configure the IP address of the TACACS+ server for the group server.

Use the **no** form of this command to remove the TACACS+ server.

server { *ipv4-address* | *ipv6-address* }

no server { *ipv4-address* | *ipv6-address* }

Parameter	Parameter	Description
Description	<i>ipv4-address</i>	IPv4 address of the TACACS+ server
	<i>ipv6-address</i>	IPv6 address of the TACACS+ server

Defaults No TACACS+ server is configured by default.

Command TACACS+ server group configuration mode

Mode

Usage Guide You must configure the **aaa group server tacacs+** command before configuring this command. To configure server address in TACACS+ group server, you must use the **tacacs-server host** command in global configuration mode. If there is no response from the first host entry, the next host entry is tried.

Configuration Examples The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group.

```
Ruijie(config)#aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs)# server 1.1.1.1
```

Related Commands	Command	Description
	aaa group server tacacs+	Configures a TACACS+ server group.

Platform N/A

Description

3.6 show tacacs

Use this command to display the TACACS+ server configuration.

show tacacs

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the TACACS+ server configuration.

Examples

```
Ruijie# show tacacs
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Related Commands	Command	Description
	tacacs-server host	Defines a TACACS+ secure server host.

Platform Description N/A

3.7 tacacs-server host

Use this command to configure a TACACS+ host.

Use the **no** form of this command to remove the TACACS+ host.

tacacs-server host [**oob** [**via** *mgmt-name*]] { *ipv4-address* | *ipv6-address* } [**port** *integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]

no tacacs-server host { *ip-address* | *ipv6-address* }

Parameter Description	Parameter	Description
	<i>ip-address</i>	IPv4 address of the TACACS+ host
	<i>ipv6-address</i>	IPv6 address of the TACACS+ host
	oob [via <i>mgmt-name</i>]	Specifies an MGMT port as the source port for TACACS+ communication.
	port <i>integer</i>	Port number of the server. The range is from 1 to 65,535. The default is 49.
	timeout <i>integer</i>	Timeout time of TACACS+ host. The range is from 1 to 1,000.

key <i>string</i>	Configures an authentication and encryption key. The value can be 0 or 7. 0 indicates no encryption, while 7 indicates simple encryption. The default is 0.
--------------------------	--

Defaults No TACACS+ host is specified by default.

Command Mode Global configuration mode

Usage Guide The TACACS+ host must be configured to implement AAA security service. You can use this command to configure one or multiple TACACS+ hosts.

Configuration Examples The following example configures a TACACS+ host.

```
Ruijie(config)# tacacs-server host 192.168.12.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.8 tacacs-server key

Use this command to configure the authentication encryption key used for TACACS+ communications between the access server and the TACACS+ server.

Use the **no** form of this command to remove the authentication encryption key.

tacacs-server key [0 | 7] string

no tacacs-server key

Parameter Description

Parameter	Description
<i>string</i>	Key string
0 7	Encryption type of key 0 indicates no encryption; 7 indicate simple encryption.

Defaults No authentication encryption key is configured by default.

Command Mode Global configuration mode

Usage Guide Use command to configure a global authentication and encryption key for TACACS+ communication. Use the **key** parameter in the **tacacs-server host** command to configure a server-based key.

Configuration The following example defines the authentication encryption key of TACACS+ server as aaa:

Examples

```
Ruijie(config)# tacacs-server key aaa
```

**Related
Commands**

Command	Description
tacacs-server host	Defines a TACACS+ host.

Platform N/A

Description

3.9 tacacs-server timeout

Use this command to set the interval for which the server waits for a server host to reply. Use the **no** form of this command to restore the default timeout interval.

tacacs-server timeout *seconds*

no tacacs-server timeout

**Parameter
Description**

Parameter	Description
<i>seconds</i>	Timeout interval in the range from 1 to 1,000 in the unit of seconds

Defaults The default is 5 seconds.

**Command
Mode** Global configuration mode

Usage Guide Use command to configure a global timeout interval. Use the **timeout** parameter in the **tacacs-server host** command to configure a server-based interval.

Configuration The following example configures the timeout interval to 10 seconds.

Examples

```
Ruijie(config)# tacacs-server timeout 10
```

**Related
Commands**

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

Platform N/A

Description

4 802.1X Commands

4.1 aaa authorization ip-auth-mode

Use this command to set the IP authorization mode.

aaa authorization ip-auth-mode { disable | supplicant | radius-server | dhcp-server | mixed }

Parameter	Parameter	Description
Description	disable	Disables IP authorization mode.
	supplicant	Enables supplicant authorization mode.
	radius-server	Enables Radius server authorization mode.
	dhcp-server	Enables DHCP server authorization mode.
	mixed	Enables mixed authorization mode.

Defaults IP authorization mode is disabled by default.

Command mode Global configuration mode

Usage Guide

Supplicant authorization mode supports only Ruijie supplicant.

Radius-server authorization mode requires the server to allocate IP addresses by framed-ip.

DHCP-server authorization mode requires the server to enable DHCP snooping or DHCP relay.

Mixed authorization mode supports multiple authorization methods.

Configuration The following example enables supplicant authentication mode.

Examples

```
Ruijie(config)# aaa authorization ip-auth-mode supplicant
```

Related Commands	Command	Description
	show running-config	Displays the IP authentication mode.

Platform N/A
Description

4.2 clear dot1x user all

Use this command to clear all the 802.1X authentication users.

clear dot1x user all

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear all the 802.1X authentication users.

Configuration The following example clears all the 802.1X authentication users.

Examples

```
Ruijie#clear dot1x user all
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.3 clear dot1x user id

Use this command to clear 802.1X authentication users according to session IDs.

clear dot1x user id *session-id*

Parameter	Parameter	Description
Description	<i>session-id</i>	Session ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear 802.1X authentication users according to session IDs.

Configuration The following example clears an 802.1X authentication user whose session ID is 12345678.

Examples

```
Ruijie#clear dot1x user id 12345678
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.4 clear dot1x user mac

Use this command to clear 802.1X authentication users according to MAC addresses.

clear dot1x user mac *mac-addr*

Parameter	Parameter	Description
Description	<i>mac-addr</i>	MAC address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear 802.1X authentication users according to MAC addresses.

Configuration The following example clears an 802.1X authentication user whose MAC address is 0012.3456.789A.

Examples Ruijie#clear dot1x user mac 0012.3456.789A

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.5 clear dot1x user name

Use this command to clear the 802.1 X authentication users according to the username.

clear dot1x user name *name-str*

Parameter	Parameter	Description
Description	<i>name-str</i>	The username of the 802.1X authentication user

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the 802.1 X authentication users according to the username.

Configuration The following example clears the 802.1X authentication user named 802.1X-user.

Examples Ruijie#clear dot1x user name dot1x-user

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.6 dot1x accounting

Use this command to configure the accounting list.

dot1x accounting *list-name*

Parameter	Parameter	Description
Description	<i>list-name</i>	The name of the accounting list

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If AAA does not adopt 802.1X accounting as the default accounting method. Use this command to configure the 802.1X accounting method.

Configuration Examples The following example configures the accounting list.

```
Ruijie(config)# dot1x accounting dot1x-acct
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.7 dot1x auth-address-table address

Use this command to configure the authentication address table.

dot1x auth-address-table address *mac-addr interface interface*

Parameter	Parameter	Description
Description	<i>mac-addr</i>	The MAC address of the authentication host
	<i>interface</i>	The interface of the authentication host

Defaults N/A

Command Mode Global configuration mode

Usage Guide Only the specified interface with the specified MAC address is able to pass the 802.1x authentication.

Configuration The following example configures the authentication address table.

Examples

```
Ruijie(config)# dot1x auth-address-table 00d0.f800.0cb2 interface
fastethernet 0/1
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.8 dot1x authentication

Use this command to configure the authentication method list.

dot1x authentication *list-name*

Parameter	Parameter	Description
Description	<i>list-name</i>	Authentication method list

Defaults N/A

Command Global configuration mode

Mode

Usage Guide If AAA does not adopt the default 802.1X authentication, use this command to configure the 802.1X authentication method.

Configuration The following example configures the authentication method list

Examples

```
Ruijie(config)# dot1x authentication dot1x-authen
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.9 dot1x auth-fail max-attempt

Use this command to set the maximum auth-attempts.

Use the **no** form of this command to restore the default setting.

dot1x auth-fail max-attempt *value*

no dot1x auth-fail max-attempt

Parameter	Parameter	Description
Description	<i>value</i>	The maximum auth-attempts
Defaults	The default is 3.	
Command Mode	Global configuration mode	
Usage Guide	Use the show dot1x command to adjust the maximum authentication attempts for those failed users.	
Configuration Examples	The following example sets the maximum auth-attempts to 2.	
Examples	<pre>Ruijie(config)# dot1x auth-fail max-attempt 2</pre>	
Related Commands	Command	Description
	show dot1x	Displays the 802.1x configuration.
Platform	N/A	
Description		

4.10 dot1x auth-mode

Use this command to specify the 802.1X authentication mode.

dot1x auth-mode { eap | chap | pap }

Parameter	Parameter	Description
Description	eap	Enables EAP-MD5 authentication mode.
	chap	Enables CHAP authentication mode.
	pap	Enables PAP authentication mode.
Defaults	The default is EAP-MD5 authentication mode.	
Command Mode	Global configuration mode	
Usage Guide	The selection of authentication mode depends on the suppliant and portal server.	
Configuration Examples	The following example enables CHAP authentication mode.	
Examples	<pre>Ruijie(config)# dot1x auth-mode chap</pre>	
Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.

Platform N/A

Description

4.11 dot1x auto-req

Use this command to configure auto-request 802.1X authentication.

Use the **no** form of this command to restore the default setting.

dot1x auto-req

no dot1x auto-req

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide Enable this function for MAB. If the authentication agent is already in the terminal system, enable it by clicking.

Configuration The following example enables auto-request 802.1X authentication.

Examples Ruijie(config)# dot1x auto-req

Related	Command	Description
Commands	show dot1x auto-req	Displays the automatic authentication request information.

Platform N/A

Description

4.12 dot1x auto-req packet-num

Use this command to set the number of auto-request authentication packets.

dot1x auto-req packet-num *num*

Parameter	Parameter	Description
Description	<i>num</i>	The number of auto-request authentication packets in the range from 0 to 1,000,000

Defaults The default is 0.

Command N/A

Mode

Usage Guide N/A

Configuration The following example sets the number of auto-request authentication packets to 100.

Examples

```
Ruijie(config)# dot1x auto-req packet-num 100
```

Related	Command	Description
Commands	<code>show dot1x auto-req</code>	Displays the authentication request information.

Platform N/A

Description

4.13 dot1x auto-req req-interval

Use this command to set the auto-request authentication interval.

Use the **no** form of this command to restore the default setting.

dot1x auto-req req-interval *time*

no dot1x auto-req req-interval

Parameter	Parameter	Description
Description	<i>time</i>	The auto-request authentication interval, in the range from 10 to 3,600 in the unit of seconds

Defaults The default is 30 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example sets the auto-request authentication interval to 50 seconds.

Examples

```
Ruijie(config)# dot1x auto-req req-interval 50
```

Related	Command	Description
Commands	<code>show dot1x auto-req</code>	Displays the authentication request information.

Platform N/A

Description

4.14 dot1x auto-req user-detect

Use this command to enable online user detection for auto-request authentication.

Use the **no** form of this command to restore the default setting.

dot1x auto-req user-detect
no dot1x auto-req user-detect

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables online user detection for auto-request authentication.

```
Ruijie(config)# dot1x auto-req user-detect
```

Related Commands	Command	Description
	show dot1x auto-req	Displays the authentication request information.

Platform Description N/A

4.15 dot1x client-probe enable

Use this command to enable online user probe function.
 Use the **no** form of this command to restore the default setting.

dot1x client-probe enable
no dot1x client-probe enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable online user probe function.

Configuration Examples The following example enables online user probe function.

```
Ruijie(config)# dot1x client-probe enable
```

Related	Command	Description
---------	---------	-------------

Commands	show dot1x	Displays 802.1X configuration.
-----------------	-------------------	--------------------------------

Platform N/A

Description

4.16 dot1x critical

Use this command to enable the server IAB (Inaccessible Authentication Bypass) on the port.
Use the **no** form of this command to restore the default setting.

dot1x critical
no dot1x critical

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This functions is disabled by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example enables the server IAB (Inaccessible Authentication Bypass) function on the port.

```
Ruijie(config-if-GigabitEthernet 0/5)#dot1x critical
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.17 dot1x critical recovery action reinitialize

Use this command to allow IAB users under the port to reinitialize authentication when the server has recovered.

Use the **no** form of this command to restore the default setting.

dot1x critical recovery action reinitialize
no dot1x critical recovery action reinitialize

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide After the port entering the inaccessible authentication bypass status, if the RADIUS server returns to normal, you need to reinitialize the authentication for all users that have accomplished the network access authorization through the inaccessible authentication bypass on ports in order to ensure the user legality.

Configuration Examples The following example allows IAB users under the port to reinitialize authentication when the server has recovered.

```
Ruijie(config-if-GigabitEthernet 0/5)#dot1x critical recovery action
reinitialize
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.18 dot1x dbg-filter

Use this command to enable debug information print for a user with a specified MAC address. Use the **no** form of this command to clear the debug information.

dot1x dbg-filter *H.H.H*

no dot1x dbg-filter *H.H.H*

Parameter Description	Parameter	Description
	<i>H.H.H</i>	The MAC address of a user

Defaults Debug information of all authentication users is printed by default.

Command mode Global configuration mode

Usage Guide Use this command to print the debug information of a specific user. If you want to locate the fault on the network where there are multiple users.

Configuration Examples The following example prints the debug information of the device with the specified MAC address.

```
Ruijie(config)# dot1x dbg-filter 00d0.f800.0001
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.19 dot1x default

Use this command to restore 802.1X configuration to the default setting.

dot1x default

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to restore 802.1X configuration for quick re-configuration.

Configuration Examples The following example restores 802.1X configuration to the default setting.

```
Ruijie(config)# dot1x default
```

Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.

Platform N/A

Description

4.20 dot1x mac-auth-bypass

Use this command to configure single MAB authentication.

Use the **no** form of this command to restore the default setting.

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command on a single dumb terminal.

Configuration The following example configures single MAB authentication.

Examples

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass
```

Related	Command	Description
Commands	show dot1x port-control interface	Displays the information about 802.1X on the interface.

Platform N/A

Description

4.21 dot1x mac-auth-bypass multi-user

Use this command to configure multiple MAB authentications.

Use the **no** form of this command to restore the default setting.

dot1x mac-auth-bypass multi-user

no dot1x mac-auth-bypass multi-user

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command when the interface is connected with multiple dumb terminals.

Configuration The following example configures multiple MAB authentications.

Examples

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass multi-user
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.22 dot1x mac-auth-bypass timeout-activity

Use this command to set the MAB authentication timeout interval.

dot1x mac-auth-bypass timeout-activity *time*

no dot1x mac-auth-bypass timeout-activity

Parameter	Parameter	Description
Description	<i>time</i>	The online time, in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 0 second.

Command Mode Interface configuration mode

Usage Guide Use this command to set the MAB authentication timeout interval for dumb terminals.

Configuration Examples The following example sets the MAB authentication timeout interval.

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass
timeout-activity 3600
```

Related Commands	Command	Description
	show dot1x port-control interface	Displays the 802.1X information.
	show dot1x port-control interface	Displays the 802.1X information.

Platform Description N/A

4.23 dot1x mac-auth-bypass violation

Use this command to configure the MAB violation.

Use the **no** form of this command to restore the default setting.

dot1x mac-auth-bypass violation

no dot1x mac-auth-bypass violation

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to configure the MAB violation on the port with only one dumb terminal in single MAB environment.

Configuration The following example configures the MAB violation.

Examples

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass violation
```

Related	Command	Description
Commands	show dot1x port-control interface	Displays the 802.1X information.

Platform N/A

Description

4.24 dot1x max-req

Use this command to set the maximum attempts of authentication requests.

dot1x max-req *num*

Parameter	Parameter	Description
Description	<i>num</i>	Maximum attempts ranging from 1 to 10.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to display the 802.1X configuration.

Configuration The following example sets the maximum attempts of authentication requests to 2.

Examples

```
Ruijie(config)# dot1x max-req 2
```

Related	Command	Description
Commands	show dot1x	Displays the information about 802.1X.

Platform N/A

Description

4.25 dot1x multi-account enable

Use this command to enable the user with one single MAC address to perform authentication with multiple accounts.

Use the **no** form of this command to restore the default setting.

dot1x multi-account enable

no dot1x multi-account enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use the command to enable the multiple-account authentication if you want to switch the username in the authentication or re-authentication, especially in the windows domain authentication.

Configuration Examples The following example enables the multiple-account authentication.

```
Ruijie(config)# dot1x multi-account enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.26 dot1x multi-mab quiet-period

Use this command to set the quiet time after the multiple MAB authentication failure.

dot1x multi-mab quiet-period *time*

Parameter	Parameter	Description
Description	<i>time</i>	Sets the quiet period after the multiple MAB authentication failure, in the range from 0 to 65,535 in the unit of seconds.

Defaults The default is 0 second, indicating no quiet period.

Command Mode Global configuration mode

Usage Guide The default setting is recommended.

Configuration Examples The following example sets the quiet period after the multiple MAB authentication failure to 2 seconds.

```
Ruijie(config)# dot1x multi-mab quiet-period 2
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

4.27 dot1x private-supPLICANT-only

Use this command to filter non-Ruijie clients.

Use the **no** form of this command to restore the default setting.

dot1x private-supPLICANT-only

no dot1x private-supPLICANT-only

	Parameter	Description
Parameter		
Description	N/A	N/A

Defaults This function disabled by default.

Command Global configuration mode

Mode

Usage Guide This command is used for authentication supporting only Ruijie clients.

Configuration The following example filters non-Ruijie clients.

Examples

```
Ruijie(config)# dot1x private-supPLICANT-only
```

	Command	Description
Related		
Commands	show dot1x private-supPLICANT-only	Displays the information about the private supplicant.

Platform N/A

Description

4.28 dot1x probe-timer alive

Use this command to set the Ruijie terminal alive interval.

dot1x probe-timer alive *time*

	Parameter	Description
Parameter		
Description	<i>time</i>	Terminal alive interval, in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 250 seconds.

Command Global configuration mode

Mode

Usage Guide If the device does not receive the probe packet from the terminal when the terminal alive interval expires, the device is considered offline. The default setting is recommended.

Configuration The following example sets Ruijie terminal alive interval to 120 seconds.

Examples

```
Ruijie(config)# dot1x probe-timer alive 120
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.29 dot1x probe-timer interval

Use this command to set the Ruijie terminal detection interval.

dot1x probe-timer interval *time*

Parameter	Parameter	Description
Description	<i>time</i>	Terminal detection interval in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 20 seconds.

Command Global configuration mode

Mode

Usage Guide The default setting is recommended.

Configuration The following example sets Ruijie terminal detection interval to 30 seconds.

Examples

```
Ruijie(config)# dot1x probe-timer interval 30
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.30 dot1x pseudo source-mac

Use this command to use a virtual MAC address as the source MAC address of the 802.1X packets sent by the device.

Use the **no** form of this command to restore the default setting.

dot1x pseudo source-mac
no dot1x pseudo source-mac

	Parameter	Description
Parameter		
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide By default, the device uses its own MAC address as the source MAC address of the EAP packets for the 802.1X authentication. Some versions of the Ruijie supplicant judge whether the access device is a Ruijie device based on the source MAC address of the EAP packets. If the access device is a Ruijie device, the supplicant device performs some private features. Configure this command if you want to enable these features.

Configuration Examples The following example uses the virtual MAC address as the source MAC address of the 802.1X packets sent by the device:

```
Ruijie(config)# dot1x pseudo source-mac
```

	Command	Description
Related Commands	N/A	N/A

Platform Description N/A

4.31 dot1x re-authentication

Use this command to enable timed re-authentication function.

Use the **no** form of the command to restore the default setting.

dot1x re-authentication
no dot1x re-authentication

	Parameter	Description
Parameter		
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command will re-authenticate the supplicant periodically after he passes the authentication. Use

the **show dot1x** command to display 802.1X configuration. The default setting is recommended.

Configuration The following example enables timed re-authentication function.

Examples

```
Ruijie(config)# dot1x re-authentication
```

Related	Command	Description
Commands	show dot1x	Displays the 802.1X information.

Platform N/A

Description

4.32 dot1x reauth-max

Use this command to set the maximum re-auth attempts.
Use the **no** form of this command to restore the default setting.

dot1x reauth-max num
no dot1x reauth-max

Parameter	Parameter	Description
Description	<i>num</i> ,	Maximum re-auth attempts. The range is from 1 to 10.

Defaults Switch: The default is 3.
Wireless: The default is 6.

Command Mode Global configuration mode

Usage Guide Use this command to specify the maximum number of supplicant re-authentications. Use the **show dot1x** command to display 802.1X configuration.

Configuration The following example sets the maximum re-auth attempts to 2.

Examples

```
Ruijie(config)# dot1x reauth-max 2
```

Related	Command	Description
Commands	show dot1x	Displays the 802.1X information.

Platform N/A

Description

4.33 dot1x redirect

Use this command to enable the second generation SU upgrade function.

Use the **no** form of this command to restore the default setting.

dot1x redirect

no dot1x redirect

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide Redirect to the supplicant software download website through the browser. See *Web Authentication Configuration Guide* for details about parameters.

Configuration The following example enables the second generation SU upgrade function,

Examples

```
Ruijie(config)# dot1x redirect
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

4.34 dot1x stationarity enable

In the port-based 802.1X control mode, dynamic users can transit freely among the ports by default.

Use this command to prevent users from transition.

Use the **no** form of this command to restore the default setting.

dot1x stationarity enable

no dot1x stationarity enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide This command must be configured before user authentication. Otherwise, you need re-authenticate all the users.

Configuration The following example prevents the user from transiting from 802.1X port to other port.

Examples

```
Ruijie(config)# dot1x stationarity enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.35 dot1x timeout quiet-period

Use this command to set the quiet period after authentication failure.

Use the **no** form of this command to restore the default setting.

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

Parameter Description	Parameter	Description
	<i>time</i>	Sets the quiet period after authentication failure, in the range from 1 to 65,535 in the unit of seconds.

Defaults The default is 10 seconds.

Command Mode Global configuration mode

Usage Guide When authentication fails, the supplicant must wait for a period of time before re-authentication.

Configuration The following example sets the quiet period after authentication failure to 60 seconds.

Examples

```
Ruijie(config)# dot1x timeout quiet-period 60
```

Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.

Platform Description N/A

4.36 dot1x timeout re-authperiod

Use this command to set the re-authentication interval when re-authentication is enabled.

dot1x timeout re-authperiod *time*

Parameter	Parameter	Description
Description	<i>time</i>	Authentication interval, in the range from 1 to 65,535 in the unit of seconds.

Defaults The default is 3,600 seconds.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to display the 802.1X configuration.

Configuration The following example sets the re-authentication interval to 2,400 seconds.

Examples

```
Ruijie(config)# dot1x timeout re-authperiod 2400
```

Related Commands	Command	Description
	show dot1x	Displays the information about 802.1X.

Platform Description N/A

4.37 dot1x timeout server-timeout

Use this command to set the server timeout interval.

dot1x timeout server-timeout *time*

Parameter	Parameter	Description
Description	<i>time</i>	The server timeout interval, in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 5 seconds.

Command Mode Global configuration mode

Usage Guide By default, the timeout of the 802.1X server is less than that of the Radius server. Use this command to raise the 802.1X timeout so as to exceed the Radius value. For details, see *Configuration Guide*.

Configuration The following example set the server timeout interval to 10 seconds.

Examples

```
Ruijie(config)# dot1x timeout server-timeout 10
```

Related	Command	Description
---------	---------	-------------

Commands	show dot1x	Displays the 802.1X information.
-----------------	-------------------	----------------------------------

Platform N/A

Description

4.38 dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant.

Use the **no** form of this command to restore the default setting.

dot1x timeout supp-timeout *time*

no dot1x timeout supp-timeout

Parameter	Parameter	Description
Description	<i>time</i>	Authentication timeout between the device and the supplicant The range is from 1 to 65,535 seconds.

Defaults The default is 3 seconds.

Command Global configuration mode

Mode

Usage Guide Use the **show dot1x** command to show display 802.1X configuration.

Configuration The following example sets the authentication timeout between the device and the supplicant to 10s:

Examples

```
Ruijie(config)# dot1x timeout supp-timeout 10
```

Related	Command	Description
Commands	show dot1x	Displays the information about 802.1x.

Platform N/A

Description

4.39 dot1x timeout tx-period

Use this command to set the request/id packet re-transmission interval.

dot1x timeout tx-period *time*

Parameter	Parameter	Description
Description	<i>time</i>	The request/id packet re-transmission interval, in range from 1 to 65,535 in the unit of seconds

Defaults Switch: The default is 3 seconds.

Command Global configuration mode
Mode

Usage Guide Use the **show dot1x** command to display 802.1X configuration.

Configuration The following example sets the request/id packet re-transmission interval to 5 seconds.

Examples

```
Ruijie(config)# dot1x timeout tx-period 5
```

Related	Command	Description
Commands	show dot1x	Displays the information about 802.1X.

Platform N/A

Description

4.40 dot1x user-name compatible

Use this command to configure the compatibility function for H3C 802.1X authentication clients and authentication servers.

Use the **no** form of this command to restore the default setting.

dot1x user-name compatible

no dot1x user-name compatible

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Enable this function when the H3C authentication client and authentication server are used for 802.1X authentication or the H3C authentication server is used for MAB authentication.

Configuration The following example configures the compatibility function for H3C 802.1X authentication clients and authentication servers.

Examples

```
Ruijie(config)# dot1x user-name compatible
```

Platform N/A

Description

4.41 dot1x valid-ip-acct enable

Use this command to enable IP address-triggered accounting.

Use the **no** form of this command to restore the default setting.

dot1x valid-ip-acct enable

no dot1x valid-ip-acct enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide Use this command to enable accounting only when users obtain valid IP addresses.

Configuration The following example enables IP address-triggered accounting.

Examples Ruijie(config)#dot1x valid-ip-acct enable

Platform N/A

Description

4.42 dot1x valid-ip-acct timeout

Use this command to configure IP address-triggered accounting timeout.

Use the **no** form of this command to restore the default setting.

dot1x valid-ip-acct timeout *time*

no dot1x valid-ip-acct timeout

Parameter	Parameter	Description
Description	<i>time</i>	IP address-triggered accounting timeout in the unit of minutes

Defaults The default is 5 minutes.

Command Global configuration mode

Mode

Usage Guide The SNMP server will not start accounting until users obtain IP addresses. In this case, use this command to configure the IP address-triggered accounting timeout.

Configuration The following example configures IP address-triggered accounting timeout.

Examples Ruijie(config)# dot1x valid-ip-acct timeout 10

Platform N/A
Description

4.43 show dot1x

Use this command to display the 802.1X setting.

show dot1x

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command

Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the 802.1X setting.

Examples

```
Ruijie#show dot1x

802.1X basic information:
 802.1X Status ..... enable
 Authentication Mode ..... eap
 Authorization mode ..... disable
 Total User Number ..... 0 (exclude dynamic user)
 Authenticated User Number ..... 0 (exclude dynamic user)
 Dynamic User Number ..... 0
 Re-authentication ..... disable
 Re-authentication Period ..... 3600 seconds
 Re-authentication max ..... 3 times
 Quiet Period ..... 10 seconds
 Tx Period ..... 30 seconds
 Supplicant Timeout ..... 3 seconds
 Server Timeout ..... 5 seconds
 Maximum Request ..... 3 times
 Client Online Probe ..... disable
 Eapol Tag ..... enable
 802.1x redirect ..... disable
 Private supplicant only ..... disable
```

Related	Command	Description
---------	---------	-------------

Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.

Platform N/A

Description

4.44 show dot1x auth-address-table

Use this command to display 802.1X authentication address table.

show dot1x auth-address-table [**address** *addr* | **interface** *interface*]

Parameter	Parameter	Description
Description	<i>addr</i>	Physical IP address that can be authenticated
	<i>interface</i>	Interface number

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the 802.1X authentication address table.

Examples

```
Ruijie #show dot1x auth-address-table
Interface      Address
-----
Fa0/1          00d0.f800.0c0e
Fa0/2          001a.c800.0102

Ruijie #show dot1x auth-address-table interface fastEthernet 0/1
Interface      Address
-----
```

```

Fa0/1          00d0.f800.0c0e

Ruijie #show dot1x auth-address-table address 00d0.f8.00.0c0e
Interface      Address
-----
Fa0/1          00d0.f800.0c0e

```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1x authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform N/A

Description

4.45 show dot1x auto-req

Use this command to display the auto-request authentication information.

show dot1x auto-req

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the auto-request authentication information.

Examples

```

Ruijie# show dot1x auto-req
Auto-Req: Enabled

```

```
User-Detect : Enabled
Packet-Num : 0
Req-Interval: 30 Seconds
```

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.

Platform N/A

Description

4.46 show dot1x max-req

Use this command to display the maximum number of request/challenge packet transmission.

show dot1x max-req

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the maximum number of request/challenge packet transmission.

```
Ruijie#show dot1x max-req
```

```
Max-Req: 3 Times
```

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.

Platform N/A

Description

4.47 show dot1x port-control

Use this command to display the port-control information.

show dot1x port-control [**interface** *interface-type interface-number*]

Parameter	Parameter	Description
Description	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface ID

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the port-control information.

```
Ruijie#show dot1x port-control
Interface Mode      Dynamic-User Static-User Max-User  Authened MAB
-----
Gi0/5   mac-based  0          0          unlimited no      disable
```

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.

dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform N/A

Description

4.48 show dot1x private-supPLICANT-only

Use this command to display the information about the private supplicant.

show dot1x private-supPLICANT-only

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the information about the private supplicant:

Examples

```
Ruijie#show dot1x private-supPLICANT-only

private-supPLICANT-only: Disabled
```

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.

dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform N/A

Description

4.49 show dot1x probe-timer

Use this command to display the configuration of online user probe.

show dot1x probe-timer

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the configuration of online user probe.

Examples Ruijie#show dot1x probe-timer

```
Hello Interval : 20
```

```
Hello Alive : 60
```

Field Description

Command	Description
Hello Interval	Sets the probe period.
Hello Alive	Sets the probe alive interval.

Related Commands	Command	Description
	N/A	N/A.

Platform N/A

Description

4.50 show dot1x re-authentication

Use this command to display re-authentication status.

show dot1x re-authentication

	Parameter	Description
Parameter	N/A	N/A
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays re-authentication status.

Examples

```
Ruijie#show dot1x re-authentication

Reauth-Enabled: Disabled
```

Command	Description
Reauth-Enabled	Whether to enable re-authentication.

	Command	Description
Related Commands	N/A	N/A

Platform Description N/A

4.51 show dot1x reauth-max

Use this command to display the maximum re-auth attempts.

show dot1x reauth-max

	Parameter	Description
Parameter	N/A	N/A
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the maximum re-authentication attempts.

Examples Ruijie#show dot1x reauth-max

```
Reauth-Max: 3 Times
```

Command	Description
Reauth-Enabled	Sets the maximum re-authentication attempts.

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

4.52 show dot1x summary

Use this command to display the 802.1X authentication summary.

show dot1x summary

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

**Command
Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide It is convenient to display the 802.1X authentication summary according to the MAC address or username.

Configuration The following example displays the summary of 802.1X authentication.

Examples Ruijie#show dot1x summary

```
ID      User      MAC          Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time
-----
-----
```

**Related
Commands**

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.

dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform N/A

Description

4.53 show dot1x timeout quiet-period

Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

show dot1x timeout quiet-period

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

Configuration Examples The following example shows how to displays the quiet period the time for the device to wait before re-authentication after the authentication failure.

```
Ruijie#show dot1x timeout quiet-period
```

```
Quiet-Period: 10 Seconds
```

Parameter Description:

Parameter	Description
Quiet-Period	The time for the device to wait before re-authentication after the authentication failure.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.54 show dot1x timeout re-authperiod

Use this command to display the re-authentication interval.

show dot1x timeout re-authperiod

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the re-authentication interval.

Configuration The following example displays the re-authentication interval.:

Examples Ruijie#show dot1x timeout re-authperiod

```
Reauth-Period: 3600 Seconds
```

Parameter Description:

Parameter	Description
Reauth-Period	Re-authentication interval.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.55 show dot1x timeout server-timeout

Use this command to display the authentication timeout period.

show dot1x timeout server-timeout

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the authentication timeout period.

Configuration Use this command to display the authentication timeout period:

Examples Ruijie#show dot1x timeout server-timeout

```
Server-Timeout: 5 Seconds
```

Parameter Description:

Parameter	Description
Server-Period	AuthenticationServer timeout periodinterval.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.56 show dot1x timeout supp-timeout

Use this command to display the request/challenge packets re-transmission interval.

show dot1x timeout supp-timeout

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the request/challenge packets re-transmission interval.

Configuration Use this command to display the request/challenge packets re-transmission interval:

Examples Ruijie#show dot1x timeout supp-timeout

```
Supp-Timeout: 3 Seconds
```

Field Description:

Field	Description
Server-Period	The request/challenge packets re-transmission interval.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.57 show dot1x timeout tx-period

Use this command to display the request/id packets re-transmission interval.

show dot1x timeout tx-period

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the request/id packets re-transmission interval.

Configuration Use this command to display the request/ id packets re-transmission interval:

```
Ruijie#show dot1x timeout tx-period

Tx-Period: 30 Seconds
```

Parameter Description:

Parameter	Description
Tx-Period	Request/id packets re-transmission interval.

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.58 show dot1x user id

Use this command to display the information about 802.1X authentication users based on user IDs.

show dot1x user id id

Parameter Description	Parameter	Description
	<i>id</i>	User ID

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its ID.

Configuration Examples The following example displays the information about the 802.1X authentication user according to the user ID.

```
Ruijie#show dot1x user id 16777225

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aaaa.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
  user acl-name ts-user_6_0_0 :
Parameter Description:
```

Parameter	Description
User name	User name
User id	User ID
Type	User type
Mac address	User's MAC address
Vlan id	User VLAN ID
Access from port	The port that user accesses from
Time online	User online time
User ip address	User IP address
Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time
Supplicant is private	Whether the terminal is a Ruijie device
Start accounting	The accounting is enabled
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.

IP privilege	The IP privilege level
user acl-name	The ACL information

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.59 show dot1x user mac

Use this command to display the information about 802.1X authentication users based on MAC addresses.

show dot1x user mac *mac-addr*

Parameter	Parameter	Description
Description	<i>mac-addr</i>	MAC address

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its MAC address.

Configuration Examples The following example displays the information about the 802.1X authentication user according to the user's MAC address.

```
Ruijie#show dot1x user mac 0023.aaaa.4286
```

```
User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aaaa.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
```

```
IP privilege is 0
user acl-name ts-user_6_0_0 :
```

Parameter Description:

Parameter	Description
User name	User name
User id	User ID
Type	User type
Mac address	User's MAC address
Vlan id	User VLAN ID
Access from port	The port that user access from
Time online	User online time
User ip address	User IP address
Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time
Supplicant is private	Whether the terminal is a Ruijie device
Start accounting	The accounting is enabled.
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.
IP privilege	The IP privilege level
user acl-name	The ACL information

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.60 show dot1x user name

Use this command to display information about 802.1X authentication users based on usernames.

show dot1x user name *name*

Parameter Description	Parameter	Description
	<i>name</i>	User name

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its username.

Configuration The following example displays the information about the 802.1X authentication user according to the user name.

Examples

```
Ruijie#show dot1x user name ts-user

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name ts-user_6_0_0 :
```

Parameter Description:

Parameter	Description
User name	User name
User id	User ID
Type	User type
Mac address	User's MAC address
Vlan id	User VLAN ID
Access from port	The port that user access from
Time online	User online time
User ip address	User IP address
Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time
Supplicant is private	Whether the terminal is a Ruijie device.
Start accounting	The accounting is enabled.
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.
IP privilege	The IP privilege level.
user acl-name	The ACL information.

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

5 Web Authentication Commands

5.1 accounting

Use this command to set an accounting method for the template.

Use the **no** form of this command to restore the default setting.

accounting { *method-list* }

no accounting

Parameter Description	Parameter	Description
	<i>method-list</i>	Name of the method list

Defaults N/A

Command Mode Template configuration mode

Usage Guide The *method-list* parameter in this command should be consistent with network accounting list name configured in AAA.

Configuration Examples The following example sets the **mlist1** accounting method for the **eportalv2** template.

```
Ruijie(config.tmplt.eportalv2) # accounting mlist1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.2 authentication

Use this command to set an authentication method for the template.

Use the **no** form of this command to restore the default setting.

authentication { *method-list* }

no authentication

Parameter Description	Parameter	Description
	<i>method-list</i>	Name of the method list

Defaults	N/A
Command Mode	Template configuration mode
Usage Guide	The <i>method-list</i> parameter in this command should be consistent with the Web authentication method list configured in AAA. The first generation authentication does not support the authentication method list configuration.

Configuration The following example sets the **mlist1** authentication method for the **eportalv2** template.

Examples

```
Ruijie(config.tmplt.eportalv2)#authentication mlist1
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

5.3 bindmode

Use this command to set a binding mode for the template.

Use the **no** form of this command to restore the default setting.

bindmode { ip-mac-mode | ip-only-mode }

no bindmode

Parameter Description	Parameter	Description
	ip-mac-mode	IP+MAC mode. The device will write both the IP address information and the MAC address information into the forwarding entry.
	ip-only-mode	IP only mode. The device writes only the IP address information into the forwarding entry. On the L3 network, it is recommended to adopt this mode in case that the MAC address is inaccurate.

Defaults The default is **ip-mac-mode**.

Command Mode Template configuration mode

Usage Guide N/A

Configuration The following example adopts the IP only mode for the **eportalv2** template.

Examples

```
Ruijie(config.tmplt.eportalv2)# bindmode ip-only-mode
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

5.4 clear web-auth direct host

Use this command to clear all authentication-exempted users.

clear web-auth direct-host [range]

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all authentication-exempted users.

```
Ruijie# clear web-auth direct-host
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

5.5 clear web-auth direct-site

Use this command to clear all authentication-exempted network resources.

clear web-auth direct-site

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears all authentication-exempted network resources.

Examples Ruijie# clear web-auth direct-site

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.6 clear web-auth user

Use this command to force the user to go offline.

clear web-auth user { **all** | **ip** { *ip-address* | *ipv6-address* } | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }

Parameter Description

Parameter	Description
<i>ip-address</i>	Specifies the user's IPv4 address.
<i>ipv6-address</i>	Specifies the user's IPv6 address.
<i>mac-address</i>	Specifies the user's MAC address.
<i>name-string</i>	Specifies the user name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example forces all users to go offline.

Examples Ruijie(config) clear web-auth user all

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.7 http redirect direct-arp

Use this command to set the address range of the authentication-exempted ARP.

Use the **no** form of this command to restore the default setting.

http redirect direct-arp { *ip-address* [*ip-mask*] }

no http redirect direct-arp { *ip-address* [*ip-mask*] }

Parameter Description

Parameter	Description
<i>ip-address</i>	IPv4 address
<i>ip-mask</i>	(Optional) IPv4 mask

Defaults No authentication-exempted ARP resource is configured by default.

Command Global configuration mode

Mode

Usage Guide The user cannot learn the ARPs of devices such as the gateway with the ARP CHECK function enabled. Use this command to enable the device to learn the ARP within a specified IP address range without authentication.

Configuration The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource.

Examples Ruijie(config)# http redirect direct-arp 172.16.0.1

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.8 http redirect direct-site

Use this command to set the range of authentication-exempted network resources.

Use the **no** form of this command to restore the default setting.

http redirect direct-site { *ipv6-address* | *ipv4-address* [*ip-mask*] [**arp**] | *mac-address* | range *startip-address* *endip-address* } [*description* *description-str*] [*group* *group-name*]

no http redirect direct-site { *ipv6-address* | *ipv4-address* [*ip-mask*] | *mac-address* | range *startip-address* *endip-address* }

Parameter Description	Parameter	Description
	<i>ipv6-address</i>	IPv6 address of the authentication-exempted network resources
	<i>ip-address</i>	IPv4 address of the authentication-exempted network resources
	<i>ip-mask</i>	IPv4 address mask of the authentication-exempted network resources (optional)
	arp	If the ARP Check is enabled on the access device, the keyword arp is needed for ARP binding of the authentication-exempted network resources (optional). It is necessary for IPv4 network resources only.
	<i>mac-address</i>	MAC address of the authentication-exempted user
	<i>startip-address</i>	Start IP address of the range of the authentication-exempted network resources
	<i>endip-address</i>	End IP address of the range of the authentication-exempted network resources
	<i>group-name</i>	Group where the authentication-exempted network resources belong
	<i>description-str</i>	Description of the authentication-exempted network resources

Defaults No authentication-exempted network resource is set.

Command Mode Global configuration mode

Usage Guide When Web/802.1x authentication is enabled, all users must pass Web/client authentication to access network resources. This command is used to make certain network resources available to unauthenticated users. All users can access the authentication-exempted Web sites. Up to 50 authentication-exempted users are supported.

Configuration Examples The following example sets the Web site with IP address 172.16.0.1 as the authentication-exempted resource.

```
Ruijie(config)# http redirect direct-site 172.16.0.1
```

The following example sets the Web site with MAC address 0000:5e00:0101 as the authentication-exempted resource.

```
Ruijie(config)# http redirect direct-site 0000:5e00:0101
```

The following example sets the range of the authentication-exempted network resources from 10.0.0.1 to 12.0.0.1.

```
Ruijie(config)# http redirect direct-site range 10.0.0.1 12.0.0.1
```

Related Commands	Command	Description
	show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

5.9 http redirect port

Use this command to redirect users' HTTP redirection request to a certain destination port.

Use the **no** form of this command to restore the default setting.

http redirect port *port-num*

no http redirect port *port-num*

Parameter Description	Parameter	Description
	<i>port-num</i>	Destination port of the HTTP request

Defaults The default is port 80.

Command Mode Global configuration mode

Usage Guide When you access the network resource, you send HTTP packets. The access device can intercept such HTTP packets to detect your access. If the access device detects that an unauthenticated user is accessing the network resource, it stops the users with an authentication page/client download page.

By default, the access device intercepts users' HTTP packets with port 80 to check whether they are accessing network resources.

This command is used to change the destination port of HTTP packets that are intercepted by the access device.

Up to 10 ports can be configured, including port 80.

Configuration The following example redirects users' HTTP requests with port 8080.

Examples Ruijie(config)# http redirect port 8080

The following example does not redirect users' HTTP requests with port 80.

Ruijie(config)# no http redirect port 80

Related Commands	Command	Description
	show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

5.10 http redirect session-limit

Use this command to set the total number of HTTP sessions that can be originated by an unauthenticated user, or the maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port.

Use the **no** form of this command to restore the default setting.

http redirect session-limit *session-num* [**port** *port-session-num*]

no http redirect session-limit

Parameter Description	Parameter	Description
	<i>session-num</i>	Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255.
	<i>port-session-num</i>	The maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port, in the range from 1 to 65535.

Defaults Totally 255 HTTP sessions can be originated by an unauthenticated user, and 300 HTTP sessions that can be originated by an unauthenticated user connected to each port.

Command Mode Global configuration mode

Usage Guide To prevent HTTP attacks caused by unauthenticated users from using up the TCP connections of the access device, the maximum number of HTTP sessions by unauthenticated users must be limited on the access device.

In addition to authentication, other programs may also occupy HTTP sessions. Therefore, it is not recommended that the maximum number of HTTP sessions by unauthenticated users be 1

Configuration Examples The following example sets the maximum number of HTTP sessions originated by an unauthenticated user to 4.

```
Ruijie(config)# http redirect session-limit 4
```

Related Commands	Command	Description
	show http redirect	Displays the HTTP redirection configuration.

Platform Description N/A

5.11 http redirect timeout

Use this command to set the timeout for the redirection connection maintenance.

Use the **no** form of this command to restore the default setting.

http redirect timeout *seconds*

no http redirect timeout

Parameter Description	Parameter	Description
--------------------------	-----------	-------------

<i>seconds</i>	Set the timeout for the redirection connection maintenance, in the range from 1 to 10 in the unit of seconds.
----------------	---

Defaults The default is 3 seconds.

Command Mode Global configuration mode

Usage Guide This command is used to set the timeout for the redirection connection maintenance. After the three-way handshake succeeds, the redirection connection is maintained until the user sends an HTTP GET/HEAD packet and the system returns an HTTP redirection packet. This timeout is set to prevent users from occupying TCP connections for long without sending any GET/HEAD packets.

Configuration Examples The following example sets the timeout for the redirection connection maintenance to 4 seconds.

```
Ruijie(config)# http redirect timeout 4
```

Related Commands	Command	Description
		show http redirect

Platform Description N/A

5.12 ip

Use this command to set an IP address for the portal server.

Use the **no** form of this command to restore the default setting.

port { *ip-address* }

no port

Parameter Description	Parameter	Description
		<i>ip-address</i>

Defaults No IP address is set for the portal server by default.

Command Mode Template configuration mode

Usage Guide This command takes place of the **http redirect** [*ip-address*] command, which is now hidden as a compatible command.

Configuration Examples The following example sets the IP address of the eportalv1 template to 172.16.0.1.

```
Ruijie(config.tmplt.eportalv1)#ip 172.16.0.1
```

```
Ruijie (config.tmplt.eportalv1) #
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

5.13 ip portal source-interface

Use this command to specify a communication port for the portal server.

Use the **no** form of this command to restore the default setting.

ip portal source-interface *interface-type interface-num*

no ip portal source-interface

**Parameter
Description**

Parameter	Description
<i>interface-type</i>	Port type
<i>interface-num</i>	Port No.

Defaults No communication interface is specified by default.

Command Global configuration mode
Mode

Usage Guide N/A

Configuration The following example specifies an aggregate port as the communication port.

Examples

```
Ruijie (config)# ip portal source-interface Aggregateport 1
```

Platform N/A
Description

5.14 port

Use this command to set a surveillance port for the portal server.

Use the **no** form of this command to restore the default setting.

port { *port-num* }

no port

**Parameter
Description**

Parameter	Description
-----------	-------------

<i>port</i>	The surveillance port of the portal server, which is on only the 2nd generation portal server,
-------------	--

Defaults The default is 50100 based on the UDP protocol.

Command Mode Template configuration mode

Usage Guide N/A

Configuration Examples The following example sets the surveillance port number of the eportalv2 server to 10000.

```
Ruijie(config.tmplt.eportalv2)#port 10000
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.15 redirect

Use this command to set the redirect packet protocol.

Use the **no** form of this command to restore the default setting.

redirect { *http* | *js* }

no redirect

Parameter Description	Parameter	Description
	<i>http</i>	HTTP 302
	<i>js</i>	HTTP 200

Defaults The default is HTTP 200.

Command Mode Template configuration mode

Usage Guide N/A

Configuration Examples The following example sets the redirect packet protocol to HTTP 200.

```
Ruijie(config.tmplt.eportalv2)#redirect http
```

Related Commands	Command	Description

N/A	N/A
-----	-----

Platform N/A

Description

5.16 show web-auth control

Use this command to display the authentication configuration.

show web-auth control

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration Examples The following example displays the authentication configuration and statistics information on the interface.

```
Ruijie(config)#show web-auth control
Port                Control  Server Name          Online User Count
-----
GigabitEthernet 0/1  On      <not configured>    0
Ruijie(config)#
```

Field	Description
Port	Name of the authentication port.
Control	Displays whether the Web authentication is enabled on the port or not.
Server Name	The customized server name on the port. <not configured> indicates the server name has not been configured.
Online User Count	The number of online users on this port.

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

5.17 show web-auth direct-arp

Use this command to display the address range of the authentication-exempted ARP.

show web-auth direct-arp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide | N/A

Configuration The following example displays the address range of the authentication-exempted ARP.

Examples

```
Ruijie(config)#show web-auth direct-arp
Direct arps:
  Address      Mask
  -----
  1.1.1.1      255.255.255.255
  2.2.2.2      255.255.255.255
Ruijie(config)#
```

Field	Description
Address	IPv4 address.
Mask	IPv4 mask.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.18 show web-auth direct-host

This command is used to display the Web authentication-exempted users.

show web-auth direct-host

Parameter	Parameter	Description
-----------	-----------	-------------

Description		
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the Web authentication-exempted users.

Examples

```
Ruijie# show web-auth direct-host
Direct hosts:
  Address           Mask                Port                ARP Binding
  -----
  192.168.0.1       255.255.255.255    Fa0/2               On
  192.168.4.11     255.255.255.255    Fa0/10              On
  192.168.5.0       255.255.255.0      Fa0/16              Off
```

Field	Description
Address	IP address of the user free of authentication
Mask	IP address mask of the user free of authentication
Port	Access device port that is bound with the user's IP address
ARP Binding	Enable/Disable ARP binding

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.19 show web-auth direct site

Use this command to display the range of the Web authentication-exempted network resources.

show web-auth direct-site [range]

Parameter Description	Parameter	Description
	N/A	N/A

Defaults No network resource without authentication is set.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the range of the Web authentication-exempted network resources without authentication.

```
Ruijie(config)#show web-auth direct-site
Direct sites:
  Address      Mask          ARP Binding Group  Description
  -----
  1.1.1.1     255.255.255.255 Off                N/A
  2.2.2.2     255.255.255.255 On                 N/A
Ruijie(config)#
```

Field	Description
Address	IP address.
Mask	IP mask.
ARP Binding	Displays whether the ARP binding function is enabled.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.20 show web-auth parameter

Use this command to display the HTTP redirect configuration.

show web-auth parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the HTTP redirect configuration

Examples

```
Ruijie# show web-auth parameter
```

```
session-limit: 10
```

```
timeout:      5
```

Field	Description
session-limit	Total number of HTTP sessions that are created by an unauthenticated user.
timeout	Timeout interval of the redirection connection.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.21 show web-auth portal-check

Use this command to display the portal-check configuration.

show web-auth portal-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the portal-check configuration.

Examples

```
Ruijie#sh web portal-check
```

```
Check:      Enable
```

```
Interval:   3s
```

```
Timeout:    5s
```

```
Retransmit: 3
```

```
Escape:     Enable
```

```
Nokick:     Disable
```

Platform N/A
Description

5.22 show web-auth rdport

Use this command to display the TCP interception port.

show web-auth rdport

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the TCP interception port.

Examples

```
Ruijie#show web-auth rdport
Rd-Port:
80 443
Ruijie#
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

5.23 show web-auth syslog ip

Use this command to display online and offline records about users.

show web-auth syslog ip ip-address

Parameter Description	Parameter	Description
	<i>ip-address</i>	A user's IP address.

Defaults N/A

Command Privileged EXEC mode
Mode

Usage Guide This command cannot be used to save original data after hot backup.

Configuration The following example displays online and offline records of users.

Examples

```
Ruijie#show web-auth syslog ip 192.168.197.35
Address: 192.168.197.35 Core-index 0 Current index 2
Index:          0
Time:           2015-10-16 20:37:34
Behavior:       ONLINE
Mac:           00d0.f822.33e7
Vid:           101
Port:          Gi3/1
Timeused:      0d 00:00:00
Flow_up:       0
Flow_down:     0

Index:          1
Time:           2015-10-16 20:42:08
Behavior:       OFFLINE
Mac:           00d0.f822.33e7
Vid:           101
Port:          Gi3/1
Timeused:      0d 00:04:27
Flow_up:       2107872
Flow_down:     2108224
```

Field	Description
Index	The number of the record.
Time	Time when the record is made.
Behavior	Online or offline behavior.
MAC	The Mac address of a user.
Vid	The VLAN ID of a user.
Port	The user port.
Timeused	The time when a user gets online.
Flow UP	The uplink traffic of a user.
Flow down	The downlink traffic of a user.

**Related
Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

Platform N/A

Description

5.24 show web-auth template

Use this command to display the portal server configuration.

show web-auth template

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide Use this command to display the portal server configuration.

Configuration The following example displays the port server configuration.

Examples

```
Ruijie#show web-auth template
Webauth Template Settings:
-----
Name:      eportalv1
Url:       http://17.17.1.21:8080/eportal/index.jsp
Ip:        17.17.1.21
BindMode:  ip-mac-mode
Type:      v1
-----
Name:      eportalv2
Url:       http://17.17.1.21:8080/eportal/index.jsp
Ip:        17.17.1.21
BindMode:  ip-only-mode
Type:      v2
Port:      50100
Acctmlist:
Authmlist:
Ruijie#
```

Field	Description
Name	Template name.
Url	Server homepage address.

Ip	Server IP address.
Type	Server type, including the first generation portal server v1, the second generation portal server v2
Port	The protocol packet communication port of the server, which is on only the second generation portal server.
Acctmlist	Accounting method list name
Authmlist	Authentication method list name

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

5.25 show web-auth user

Use this comma to display the online information, including IP address, interface, and online duration, of all users or the specified users.

show web-auth user { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-strin* }

**Parameter
Description**

Parameter	Description
<i>ip-address</i>	IPv4 address of the user.
<i>mac-address</i>	MAC address of the user.
<i>name-string</i>	User name.

Defaults N/A

**Command
Mode** Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the global Web authentication configuration and statistics.

Examples

```
Ruijie# show web-auth user all
Current user num : 4, online 2

Address          Online   Time Limit   Time Used   Status   Name
-----
192.168.0.11    On      0d 01:00:00  0d 00:15:10 Active
192.168.0.13    On      0d 01:00:00  0d 00:00:59 Active   111
```



```

192.168.0.25 Off 0d 01:00:00 0d 00:00:59 Create
192.168.0.46 Off 0d 01:00:00 0d 01:00:00 Destroy 222

```

```
Ruijie# show web-auth user ip 192.168.0.11
```

```

Address      : 192.168.0.11
Mac          : 00d0.f800.2233
Port         : Gi0/2
Online       : On
Time Limit   : 0d 01:00:00
Time Used    : 0d 00:15:10
Time Start   : 2009-02-22 20:05:10
Status       : Active

```

Field	Description
Address	IP address of the user
Mac	MAC address of the user
Port	Access device port connected to the user
Online	Whether the user is online
Time Limit	Available duration of the user. 0 means unlimited.
Time Used	Online duration of the user
Time Start	Time when the user passes authentication and gets online
Status	User status. Active means the user is normally online, Create means the user is created without any settings, Destroy means the user is deleted with its settings not cleared.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.26 url

Use this command to set the portal server URL.

Use the **no** form of this command to restore the default setting.

url *url-string*

no url

Parameter Description

Parameter	Description
<i>url-string</i>	Portal server URL, starting with http:// or https:// . The maximum length of this address is 255 bytes.

Defaults No portal server URL is set by default.

Command Mode Template configuration mode

Usage Guide This command takes place of the **http redirect homepage [url-string]** command, which is now hidden as a compatible command.,
If no URL is specified, the default URL in the **http://[ip-address]** format will be adopted, among which **ip-address** is the IP address of the server.

Configuration The following example sets the eportalv1 template URL to **http://www.web-auth.net/login**.

Examples

```
Ruijie(config.tmplt.eportalv1)#url http://www.web-auth.net/login
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.27 web-auth accounting jitter-off

Use this command to enable jitter-off accounting function.

Use **no** form of this command to restore the default setting.

web-auth accounting jitter-off

no web-auth accounting jitter-off

Parameter Description

Parameter	Description
N/A	N/A

Defaults Jitter-off accounting function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example enables jitter-off accounting function.

Examples

```
Ruijie (config)# web-auth accounting jitter-off
```

Platform N/A

Description

5.28 web-auth accounting v2

Use this command to specify an accounting method.

Use **no** form of this command to restore the default setting.

web-auth accounting v2 { default | name }

no web-auth accounting v2 { default | name }

Parameter Description	Parameter	Description
	<i>name</i>	The accounting method

Defaults No accounting method is specified by default.

Command Mode Global configuration mode/Template configuration mode

Usage Guide N/A

Configuration The following example specifies an accounting method.

Examples Ruijie (config.tmplt.eportalv2)# web-auth accounting v2 default

Platform Description N/A

5.29 web-auth authentication v2

Use this command to specify an authentication method.

Use **no** form of this command to restore the default setting.

web-auth authentication v2 [default | name]

no web-auth authentication v2 [default | name]

Parameter Description	Parameter	Description
	<i>name</i>	The authentication method

Defaults The default method is the same as AAA.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example specifies an authentication method.

Examples

```
Ruijie (config.tmplt.eportalv2)# web-auth authentication v2 default
```

Platform N/A
Description

5.30 web-auth direct-host

Use this command to set the authentication-exempted IP/MAC address range.

Use the **no** form of this command to restore the default setting.

web-auth direct-host { *ip-address* [*ip-mask*] [**arp**] | *mac-address* } [**port** *interface-name*]

no web-auth direct-host { *ip-address* [*ip-mask*] | *mac-address* }

Parameter Description	Parameter	Description
	<i>ip-address</i>	IPv4 address of authentication-exempted user
	<i>ip-mask</i>	Mask of the IPv4 address free of authentication (optional).
	port <i>interface-name</i>	Binds user's IP address with a port of the access device (optional).
	arp	If ARP CHECK is enabled on the access device, keyword arp is needed for ARP binding of the IP address used by users free of authentication (optional). It is necessary for IPv4 addresses only.
	<i>mac-address</i>	MAC address of authentication-exempted user
	<i>mac-address</i>	MAC address of the authentication-exempted user
	<i>startip-address</i>	Start IP address of the range of the authentication-exempted network resources
	<i>endip-address</i>	End IP address of the range of the authentication-exempted network resources
	<i>group-name</i>	Group where the authentication-exempted network resources belong

Defaults No user is exempted from authentication. All users must pass the Web authentication to access the restricted network resources.

Command Mode Global configuration mode

Usage Guide When a user is set to be exempted from authentication, it can access all reachable network resources without Web authentication.
 Up to 50 users can be set to be exempted from authentication.

Configuration Examples The following example sets the user with the IP address 172.16.0.1 to be exempted from authentication.

```
Ruijie(config)# web-auth direct-host 172.16.0.1
```

The following example sets the user with the MAC address 0000:5e00:0101 to be exempted from

authentication.

```
Ruijie(config)# web-auth direct-host 0000:5e00:0101
```

Related Commands

Command	Description
show web-auth direct-host	Displays the users free of Web authentication.

Platform N/A

Description

5.31 web-auth enable

Use this command to enable the Web authentication function on a port. This command is compatible with the **web-auth port-control** command.

Use the **no** form of this command to restore the default setting.

web-auth enable

no web-auth enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The Web authentication function is disabled on the port by default.

The **default** template is eportalv1.

Command Mode

Interface configuration mode

Usage Guide

To ensure the Web authentication function, the authentication page URL should be configured.

Because template applications are integrated into the controlled switch, the template or the server applications of the interface where the Web authentication function is disabled will be automatically cleared. This command is compatible with the original command that used to apply the template or server application in the global configuration mode.

Configuration Examples

The following example enables the Web authentication function on gigabitEthernet 0/14.

Examples

```
Ruijie(config)# interface GigabitEthernet 0/14
Ruijie(config-if-GigabitEthernet 0/14)# web-auth enable
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.32 web-auth logging enable

Use this command to enable the Web authentication syslog function.

Use the **no** form of this command to restore the default setting.

web-auth logging enable { *num* }

no web-auth logging enable

Parameter Description	Parameter	Description
	<i>num</i>	The syslog printing rate, indicating how many syslog entries can be printed in a second. The value is in the range from 0 to 65535. 0 indicates no limit.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to limit the syslog printing rate for only the functional module.

Configuration Examples The following example enables the syslog printing with no rate limit.

```
Ruijie(config)# web-auth logging enable 0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.33 web-auth portal key

Use this command to set the communication key between the access device and the authentication server.

Use the **no** form of this command to clear the communication key between the redirected Web request of a user and the authentication server.

web-auth portal key *key-string*

no web-auth portal key

Parameter Description	Parameter	Description
	<i>key-string</i>	Communication key between the access device and the authentication server. The maximum length of the key is 255 bytes.

- Defaults** No key is set by default.
- Command Mode** Global configuration mode
- Usage Guide** To use the Web authentication function, the communication key between the access device and the authentication server must be set.

Configuration Examples The following example sets the communication key between the access device and the authentication server to web-auth.

```
Ruijie(config)# web-auth portal key web-auth
```

Related Commands

Command	Description
http redirect	Sets the IP address of the authentication server.
http redirect homepage	Sets the address of the authentication homepage.
web-auth port-control	Enables the Web authentication on the port.

Platform N/A

Description

5.34 web-auth portal-check

Use this command to enable portal server check.

Use the **no** form of this command to restore the default setting.

web-auth portal-check [**interval** *intsec*] [**timeout** *tosec*] [**retransmit** *retires*]
no web-auth porta-check

Parameter Description

Parameter	Description
<i>intsec</i>	Check interval in the range from 1 to 1,000 in the unit of seconds. The default is 10 seconds.
<i>tosec</i>	Timeout interval in the range from 1 to 1,000 in the unit of seconds. The default is 5 seconds.
<i>retires</i>	Retry count in the range from 1 to 100. The default is 3.

Defaults Portal server check is disabled by default.

Command Mode Global configuration mode

Usage Guide It is recommended to use this command when there are multiple servers.

Configuration The following example enables portal server check.

Examples

```
Ruijie (config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

Platform
Description N/A

5.35 web-auth portal-escape

Use this command to enable portal-escape function.

Use the **no** form of this command to restore the default setting.

web-auth portal-escape
no web-auth portal-escape

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command together with **web-auth portal-check** command to sustain key services when the portal server is abnormal.

Configuration The following example enables portal-escape function.

Examples

```
Ruijie (config)# web-auth portal-escape
```

Platform
Description N/A

5.36 web-auth station-move arp-detect

Use this command to disable STA-move ARP detection.

no web-auth station-move arp-detect

Use this command to restore the default setting.

default web-auth station-move arp-detect

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

Defaults The STA-move ARP detection is enabled by default.

Command Mode Global configuration mode, interface configuration mode

Usage Guide N/A

Configuration Examples The following example disables STA-move ARP detection.

```
Ruijie (config)# no web-auth station-move arp-detect
Ruijie(config-if-GigabitEthernet 2/1)# no web-auth station-move arp-detect
```

Platform Description N/A

5.37 web-auth station-move auto

Use this command to enable smart station-move function.

Use the **no** form of this command to restore the default setting.

web-auth station-move auto

no web-auth station-move auto

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables smart station-move function.

```
Ruijie (config)# web-auth station-move auto
```

Platform Description N/A

5.38 web-auth template

Use this command to create the first generation authentication template and enter its configuration

mode.

web-auth template eportalv1

Use this command to create the customized second generation authentication template and enter its configuration mode.

web-auth template { *template-name* } **v1**

Use this command to create the second generation authentication template and enter its configuration mode.

web-auth template eportalv2

Use this command to create the customized second generation authentication template and enter its configuration mode.

web-auth template { *template-name* } **v2**

Use this command to remove the template.

no web-auth template { *template-name* }

Parameter Description	Parameter	Description
	eportalv1	Applies the first generation authentication template.
	eportalv2	Applies the second generation authentication template.
	<i>template-name</i>	Sets the name of the customized authentication template.

Defaults No template is configured by default.

Command Mode Global configuration mode

Usage Guide You can enter the **eportalv1** template mode to configure the IP address and URL instead of executing the **http redirect** and **http redirect homepage** commands. The **http redirect** and **http redirect homepage** commands are compatible on the device, which will be converted to this command.

The original command **portal-server** is compatible on the device, which will be converted to this command.

To ensure the Web authentication function, configure and apply a functional portal server. The **eportalv1** template is applied by default. The IP address, the URL and the communication secret key of the **eportalv1** template should be configured. If no URL format is specified, the default **http://[ip-address]** format will be adopted. The IP address of the portal server is the network resource exempted from authentication, so the unauthenticated user can access it. The device limits the uplink traffic that accesses the IP address to prevent attacks. The upper limit is proportionate to the number of the physical ports.

Configuration The following example configures the **eportalv1** template.

Examples

```
Ruijie(config)# web-auth template eportalv1
Ruijie(config.tmplt.eportalv1)#
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

5.39 web-auth update-interval

Use this command to set the interval at which the online user information is updated.

Use the **no** form of this command to restore the default setting.

web-auth update-interval {seconds}

no web-auth update-interval

**Parameter
Description**

Parameter	Description
seconds	Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds.

Defaults

The default is 180 seconds.

**Command
Mode**

Global configuration mode

Usage Guide

N/A

Configuration

The following example sets the interval at which the online user information is updated to 60 seconds.

Examples

```
Ruijie(config)# web-auth update-interval 60
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

5.40 web-auth vlan-control

Use this command to configure the authenticable VLAN list.

Use the **no** form of this command to restore the default setting.

web-auth vlan-control *vlan-list*
no web-auth vlan-control

**Parameter
Description**

Parameter	Description
<i>vlan-list</i>	Authenticable VLAN list

Defaults The default is port-control authentication.

**Command
Mode** Interface configuration mode

Usage Guide N/A

Configuration Use this command to configure the authenticable VLAN list.

Examples Ruijie (config-if-GigabitEthernet 0/1)# web-auth vlan-control 1

**Platform
Description** N/A

6 SCC Commands

6.1 Identifier Description

Identifier	Description
vlanlist	Authentication-exemption VLAN list
interval	Authenticated-user online-status detection interval
threshold	The traffic threshold of authenticated-user online-status detection

6.2 auth-mode gateway

Use this command to change the authentication mode configured on the device from access authentication to gateway authentication.

auth-mode gateway

Use this command to change the authentication mode configured on the device from gateway authentication to access authentication.

no auth-mode gateway

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Access authentication mode

Command Mode Global configuration mode

Default Level 14

Usage Guide The core device that performs access control needs to be enabled with the gateway authentication mode.

Configuration Examples The following example changes the authentication mode configured on the device to gateway authentication.

```
Ruijie(config)# auth-mode gateway
```

```
Please save config and reload system.
```

Defaults Use the **show running** command to display the authentication mode configured on a device.

Prompt Messages N/A

Common Errors Forget to save the authentication mode configuration change before restarting the device. This error causes that the newly configured authentication mode does not take effect.

Platforms

6.3 direct-vlan

Use this command to configure authentication-exemption VLANs.

direct-vlan *vlanlist*

Use this command to delete the authentication-exemption VLAN configuration.

no direct-vlan *vlanlist*

Parameter Description	Parameter	Description
	<i>vlanlist</i>	VLAN list, which can be a VLAN or a group of VLANs.

Defaults By default, no authentication-exemption VLANs are configured.

Command Mode Global configuration mode

Default Level 14

Usage Guide You can use this command to configure authentication-exemption VLANs, so that users in specified VLANs can access the Internet without experiencing dot1x or Web authentication.

Configuration Examples The following example configures the VLAN2 as an authentication-exemption VLAN.

```
Ruijie(config)# direct-vlan 2
```

The following example configures the VLAN2 under the interface Gi 0/1 as an authentication-exemption VLAN.

```
Ruijie(config)#int gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# direct-vlan 2
```

Verification Use the **show direct-vlan** command to display the authentication-exemption VLAN configuration.

Prompt Messages N/A

Common Errors N/A

Platforms

6.4 nac-author-user maximum

Use this command to configure the limit on IPv4 user capacity on a port.

nac-author-user maximum *max-user-num*

Use this command to remove the limit on the IPv4 user capacity on a port.

no nac-author-user maximum

Parameter Description	Parameter	Description
	<i>max-user-num</i>	Defines the maximum number of IPv4 access users. The range is from 1 to 1,024.

Defaults By default, the number of IPv4 access users is not limited.

Command Mode Interface configuration mode

Default Level 14

Usage Guide Use this command to configure the maximum number of IPv4 access users on a port.

Configuration Examples The following example restricts the maximum number of IPv4 users to 100 on interface Gi 0/1.

```
Ruijie(config)#int gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#nac-author-user maximum 100
```

Verification

1. Use the **show nac-author-user** command to display the current and the maximum numbers of IPv4 access users on all ports.
2. Use the **show nac-author-user interface** *interface-name* command to display the current and the maximum numbers of IPv4 access users on the specified port.

Prompt Messages N/A

Common Errors N/A

Platforms

6.5 offline-detect interval threshold

Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specified threshold or is zero in a specified interval.

offline-detect interval *interval* **threshold** *threshold*

Use this command to restore the default user online-status detection configuration.

default offline-detect

Use this command to disable user online-status detection.

no offline-detect

Parameter Description	Parameter	Description
	<i>interval</i>	Indicates the interval of traffic detection (in minutes). The range is from 6 to 65,535 in minutes on a switch.
	<i>threshold</i>	Indicates the traffic threshold (in bytes).

Defaults By default, the detection interval is 8 hours and the traffic threshold is 0.

Command Mode Global configuration mode

Default Level 14

Usage Guide You can use this command to configure user online-status detection to enable the device to disconnect the authenticated user whose traffic is lower than a specified value and end accounting process.

Configuration Examples The following example directly disconnects a user for the user's traffic is lower than 5 Kbytes within 5 minutes.

```
Ruijie(config)#offline-detect interval 5 threshold 5120
```

Verification Use the **show running** command to display the configuration of online-status detection for authenticated users.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

6.6 show direct-vlan

Use this command to display the authentication-exemption VLAN configuration.

show direct-vlan [**interface** *interface-name*]

Parameter Description	Parameter	Description
		<i>interface-name</i>

Command Mode Privileged EXEC mode

Level 14

Usage Guide N/A

Configuration The following example displays the authentication-exemption VLAN configuration.

Examples

```
Ruijie #show direct-vlan
direct-vlan 5,7,100
```

Prompt Messages N/A

Platforms This command is supported only on switches.

6.7 show nac-author-user interface

Use this command to display the capacity limit and current number of IPv4 users on all interfaces or a specified interface.

show nac-author-user [**interface** *interface-name*]

Parameter Description	Parameter	Description
		<i>interface-name</i>

Command Mode Privileged EXEC mode

Level 14

Usage Guide N/A

Configuration Examples The following example displays the current number and capacity limit of IPv4 users on interface Gi 0/1.

```
Ruijie#show nac-author-user interface gi 0/1
Port      Cur_num  Max_num
-----  -
Gi0/1    0        100
```

Prompt Messages N/A

Platforms

6.8 station-move permit

Use this command to enable authenticated-user migration.

station-move permit

Use this command to disable authenticated-user migration.

no station-move permit

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Authenticated-user migration is not permitted by default.

Command Mode Global configuration mode

Level 14

Usage Guide You can enable the authenticated-user migration function to allow the online users to be authenticated again and get online from different physical locations (different ports or VLANs).

Configuration Examples The following examples enables authenticated-user migration.

```
Ruijie(config)#station-move permit
```

Verification Use the **show running** command to check whether the authenticated-user migration function is enabled.

Prompt Messages N/A

**Common
Errors** N/A

Platforms

7 Global IP-MAC Binding Commands

7.1 address-bind

Use this command to configure global IP-MAC address binding. Use the **no** form of this command to restore the default setting.

address-bind { *ip-address* | *ipv6-address* } *mac-address*

no address-bind { *ip-address* | *ipv6-address* } *mac-address*

Parameter	Parameter	Description
Description	<i>ip-address</i>	IPv4 address to be bound
	<i>ipv6-address</i>	IPv6 address to be bound
	<i>mac-address</i>	MAC address to be bound

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures global IP-MAC address binding.

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
```

Related Commands	Command	Description
	show address-bind	Displays the IP address-MAC address binding table.

Platform Description N/A

7.2 address-bind install

Use this command to enable a binding policy globally. Use the **no** form of this command to restore the default setting.

address-bind install

no address-bind install

Parameter	Parameter	Description
-----------	-----------	-------------

Description	N/A	N/A				
Defaults	N/A					
Command Mode	Global configuration mode					
Usage Guide	If you bind an IP address to a MAC address, run this command to make the installation policy take effect.					
Configuration Examples	The following example enables a binding policy.					
Examples	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001 Ruijie(config)# address-bind install</pre>					
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

7.3 address-bind ipv6-mode

This command is used to set the IPv6 address binding mode. Use the **no** form of this command to restore the default setting.

This command is also used to set the compatible mode.

address-bind ipv6-mode { compatible | loose | strict }

no address-bind ipv6-mode

Parameter Description	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>compatible</td> <td>Compatible mode</td> </tr> <tr> <td>loose</td> <td>Loose mode</td> </tr> <tr> <td>strict</td> <td>Strict mode</td> </tr> </tbody> </table>	Parameter	Description	compatible	Compatible mode	loose	Loose mode	strict	Strict mode
Parameter	Description								
compatible	Compatible mode								
loose	Loose mode								
strict	Strict mode								
Defaults	The default is strict mode.								
Command Mode	Global configuration mode.								
Usage Guide	N/A								
Configuration Examples	The following example configures the IPv6 address binding mode.								
Examples	<pre>Ruijie# configure terminal</pre>								

```
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind ipv6-mode compatible
```

Related Commands	Command	Description
	show address-bind uplink	Displays the exceptional port of the address binding.

Platform N/A
Description

7.4 address-bind uplink

This command is used to configure the exception port. Use the **no** form of this command to restore the default setting.

```
address-bind uplink interface-id
no address-bind uplink interface-id
```

Parameter	Parameter	Description
Description	<i>interface-id</i>	Switching port or layer 2 aggregate port.

Defaults All ports are non-exception ports by default.

Command Mode Global configuration mode.

Usage Guide If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.
 If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

Configuration The following example configures the exception port.

```
Examples Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind uplink GigabitEthernet 0/1
```

Related Commands	Command	Description
	show address-bind uplink	Displays the exceptional port of address binding.

Platform N/A
Description

7.5 show address-bind

Use this command to display global IP address-MAC address binding.

show address-bind

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays global IPv4 address-MAC address binding.

Examples

```
Ruijie#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
-----
192.168.5.1        00d0.f800.0001
```

Field	Description
Total Bind Addresses in System	IPv4 address-MAC address binding count
IP Address	Bound IP address
Binding MAC Addr	Bound MAC address

Related Commands	Command	Description
	address-bind	Enables IP address-MAC address binding.

Platform N/A

Description

7.6 show address-bind uplink

Use this command to display the exception port.

show address-bind uplink

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command mode N/A

Usage Guide N/A

Configuration The following example displays the exception port.

Examples

```
Ruijie#show address-bind uplink
Port      State
-----
Gi0/1     Enabled
Default   Disabled
```

Field	Description
Port	Short for exception ports. All ports are non-exception ports by default.
State	Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it is not.

Related

Commands

Command	Description
address-bind uplink	Sets the exception port.

Platform

N/A

Description

8 Password-Policy Commands

8.1 password policy life-cycle

Use this command to set the password lifecycle. Use the **no** form of this command to restore the default setting.

password policy life-cycle days


no password policy life-cycle

Parameter Description	Parameter	Description
	<i>days</i>	Sets the password lifecycle, in the range from 1 to 65535 in the unit of days.

Defaults No password lifecycle is set by default.

Command Mode Global configuration mode

Usage Guide This command is used to set the password lifecycle. After the password lifecycle expires, the system reminds you to change the password when you login next time.

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

Configuration Examples The following example sets the password lifecycle to 90 days.

```
Ruijie(config)# password policy life-cycle 90
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.2 password policy min-size

Use this command to set the minimum length of the password. Use the **no** form of this command to restore the default setting.

password policy min-size length


no password policy min-size

Parameter Description	Parameter	Description
		<i>length</i>

Defaults No minimum length of the password is set by default.

Command Mode Privileged EXEC mode

Usage Guide This command is used to set the minimum length of the password,

-  This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

Configuration The following example sets the minimum length of the password to 8.

Examples Ruijie(config)# password policy min-size 8

Related Commands	Command	Description
		N/A

Platform Description N/A

8.3 password policy no-repeat-times

Use this command to ban the use of passwords used in the past several times. Use the no form of this command to restore the default setting.

password policy no-repeat-times times

no password policy no-repeat-times

Parameter Description	Parameter	Description
		<i>times</i>


Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this function is enabled, passwords used in the past several times are recorded. If the

new password has been used, the alarm message is displayed and password configuration fails.

This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

Configuration The following example bans the use of passwords used in the past five times.

Examples Ruijie(config)# password policy no-repeat-times 5

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.4 password policy strong

Use this command to enable strong password check.

password policy strong

no password policy strong

Parameter Description


Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide If the following two kinds of passwords are set not matching the strength policy, the alarm message is displayed.

1. The password the same as the username.
2. The simple password containing only characters or numbers.

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

Configuration The following example configures the strong password check.

Examples Ruijie(config)# password policy strong

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.5 service password-encryption

Use this command to encrypt a password. Use the **no** form of this command to restore default setting.

service password-encryption

no service password-encryption

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is disabled by default. Various passwords are displayed in plain text, unless they are encrypted. After you run the **service password-encryption** and **show running** or **write** command to save your configuration, the password changes into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.

Configuration The following example encrypts the password:

Examples

```
Ruijie(config)# service password-encryption
```

Related Commands	Command	Description
	enable password	Sets passwords of different privileges.

Platform Description N/A

8.6 show password policy

Use this command to display the password security policy set by the user.

show password policy

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the password security policy set by the user.

Configuration The following example displays the password security policy set by the user.

Examples

```
Ruijie#show password policy
Global password policy configurations:
Password encryption:           Enabled
Password strong-check:        Enabled
Password min-size:             Enabled (6 characters)
Password life-cycle:           Enabled (90 days)
Password no-repeat-times:      Enabled (max history record: 5)
```

Field	Description
Password encryption	Whether to encrypt the password.
Password strong-check	Whether to enable password strong-check.
Password min-size	Whether to set the minimum length of the password.
Password life-cycle	Whether to set the password lifecycle.
Password no-repeat-times	

Related Commands	Command	Description
		N/A

Platform Description N/A

9 Port Security Commands

9.1 show port-security

Use this command to display the port security configuration and the secure address.

show port-security [**address** [**interface** *interface-id*] | **binding** [**interface** *interface-id*] | **interface** *interface-id* | **all**]

Parameter Description	Parameter	Description
	address	Displays all secure addresses, or the secure address of the specified port.
	binding	Displays all port security bindings, or the port security bindings of the specified port.
	interface <i>interface-id</i>	Displays the port security configuration of the specified port.
	all	Displays all valid secure addresses and valid port security bindings.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide To display all port security configuration and violation management, execute the command without any parameter. To display the security configuration, the secure address, or the port security binding of the specified interface, execute the command with the corresponding parameter.

Configuration Examples The following example displays the port security statistics.

```
Ruijie#show port-security
NO. SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind
SecurityAction
(Count) (Count) (Count) (Count)
-----
1 Gi0/1 128 2 2 1 protect
-----
Total secure addresses in System : 2
Total secure bindings in System : 3
```

Field	Description
NO.	Serial number.

Secure Port	Port name
MaxSecureAddr(count)	The maximum number of secure addresses on the port.
CurrentAddr(count)	The current number of secure addresses on the port.
CurrentIpBind (count)	The current number of IP addresses bindings on the port.
CurrentIpMacBind (count)	The current number of IP-MAC address bindings on the port.
Security Action	Violation management.
Total secure addresses in System	The total number of secure addresses on the device.
Total secure bindings in System	The total number of port security bindings on the device,

The following example displays the port security configuration on interface GigabitEthernet 0/1.

```
Ruijie#show port-security interface gigabitEthernet 0/1
Interface           : GigabitEthernet 0/1
Port status         : down
Port Security       : enabled
SecureStatic address aging : disabled
Sticky dynamic address : disabled
Violation mode      : protect
Maximum MAC Addresses : 128
Total MAC Addresses : 2
Configured MAC Addresses : 2
Dynamic MAC Addresses : 0
Sticky MAC Addresses : 0
Total security binding : 3
IPv4-ONLY Binding Addresses : 1
IPv6-ONLY Binding Addresses : 1
IPv4-MAC Binding Addresses : 1
IPv6-MAC Binding Addresses : 0
Aging time (min)    : 0
```

Field	Description
Interface	Port name.
Port status	Port status.
Port Security	Displays whether the port security is enabled.
SecureStatic address aging	Displays whether the static secure address aging is enabled.
Sticky dynamic address	Displays whether the dynamic secure address is converted to the sticky secure address,
Violation mode	Port violation management.

Maximum MAC Addresses	The maximum number of secure addresses on the port.
Total MAC Addresses	The number of valid secure addresses on the port.
Configured MAC Addresses	The number of static secure addresses.
Dynamic MAC Addresses	The number of dynamic secure addresses.
Sticky MAC Addresses	The number of sticky secure addresses.
Total security binding	The number of valid port security bindings.
IPv4-ONLY Binding Addresses	The number of IPv4 addresses bindings.
IPv6-ONLY Binding Addresses	The number of IPv6 addresses bindings.
IPv4-MAC Binding Addresses	The number of IPv4-MAC address bindings.
IPv6-MAC Binding Addresses	The number of IPv6-MAC address bindings.
Aging time(min)	The aging time of the secure address.

The following example displays all secure addresses on the device.

```
Ruijie#show port-security address
NO.  VLAN  MacAddress      PORT                TYPE                RemainingAge (mins)
STATUS
-----
-----
1    1      00d0.f800.073c  GigabitEthernet 0/1    Configured          --
active
2    1      00d0.f800.073d  GigabitEthernet 0/1    Configured          --
active
```

Field	Description
NO.	Serial number.
Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
Type	Secure address type.
Remaining Age(mins)	The aging time of the secure address.
STATUS	The secure address status.

The following example displays all port security bindings on the device.

```
Ruijie#show port-security binding
NO.  VLAN  MacAddress      PORT      IpAddress
FilterType FilterStatus
-----
-----
1    1      00d0.f800.073c  Gi0/1     192.168.12.202      ipv4-mac
active
2    --      --              Gi0/1     192.168.0.1         ipv4-only
active
```



```
3 -- -- Gi0/1 ffaa:ddcc::1 ipv6-only
activ
```

Field	Description
NO.	Serial number.
Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
IpAddress	IP address.
FilterType	The filtering type of the port security binding.
FilterStatus	The status of the port security binding.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

9.2 switchport port-security

Use this command to configure port security and the way to deal with violation.

Use the **no** form of this command to restore the default setting.

switchport port-security [violation { protect | restrict | shutdown }]

no switchport port-security [violation]

Parameter Description

Parameter	Description
protect	Discards the packets breaching security.
restrict	Discards the packets breaching security and sends the Trap message.
shutdown	Discards the packets breaching the security, sends the Trap message and disables the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.

i If the violation handling mode is changed after violation occurs, the new mode takes effect only after the violation mode is restarted.

Configuration Examples The following example enables port security on interface gigabitethernet 1/1, and the way to deal with violation is **shutdown**:

```
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security violation shutdown
```

Related Commands

Command	Description
show port-security	Displays port security settings.

Platform Description N/A

9.3 switchport port-security aging

Use this command to set the aging time for all secure addresses on an interface.

Use the **no** form of this command to restore the default setting.

switchport port-security aging {static | time *time* }

no switchport port-security aging {static | time }

Parameter Description

Parameter	Description
static	Applies the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.
time <i>time</i>	Specifies the aging time for the secure address on this port. Its range is 0-1,440 in minutes. If you set it to 0, the aging function is disabled actually.

Defaults No secure address is aged by default.

Command Mode Interface configuration mode

Usage Guide In interface configuration mode, use the **no switchport port-security aging time** command to disable the aging for security addresses on the port. Use the **no switchport port-security aging static** command to apply the aging time to only the dynamically learned security address. Use the **show port-security** command to display configuration. When both port security and 802.1X authentication functions are enabled, 802.1X clients must get re-authenticated for network access once the secure addresses are aged.

i To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface.

Configuration Examples The following example sets the aging time for all secure addresses on interface gigabitethernet 1/1 to eight minutes.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
Ruijie(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.

Platform Description N/A

9.4 switchport port-security binding

Use these commands to configure secure address binding manually in the interface configuration mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

switchport port-security binding { *ipv4-address* | *ipv6-address* }

no switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

no switchport port-security binding { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
<i>mac-address</i>	The source MAC addresses to be bound
<i>vlan_id</i>	VLAN ID of the binding source MAC address
<i>ipv4-address</i>	Binds IPv4 addresses.
<i>ipv6-address</i>	Binds IPv6 addresses.

Defaults N/A

Command Mode Interface configuration mode

- Usage Guide**
1. For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.
 2. For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.
- Network is often accessible to static users with secure addresses without authorization. If authorization is configured, these users must comply with it.

Configuration The following example binds the IP address 192.168.1.100 on interface g 0/10:

Examples

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security binding 192.168.1.100
Ruijie(config-if)# end
```

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security binding 00d0.f800.5555 vlan 1
192.168.1.100
Ruijie(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding interface	Configures the secure address binding in privileged EXEC mode.
switchport port-security mac-address	Sets the static secure address.
switchport port-security aging	Sets the aging time for secure address.

Platform N/A

Description

9.5 switchport port-security interface binding

Use these commands to configure secure address binding manually in the privileged EXEC mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

switchport port-security interface *interface-id* **binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

switchport port-security interface *interface-id* **binding** { *ipv4-address* | *ipv6-address* }

no switchport port-security interface *interface-id* **binding** [*mac-address* **vlan** *vlan_id*]

{ *ipv4-address* | *ipv6-address* }
no switchport port-security interface *interface-id* **binding** { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
<i>interface-id</i>	Binds interface ID.
<i>mac-address</i>	Binds source MAC address.
<i>vlan_id</i>	VLAN ID of the binding source MAC address
<i>ipv4-address</i>	Binds IPv4 address.
<i>ipv6-address</i>	Binds IPv6 address .

Defaults N/A

Command Mode Global configuration mode

Usage Guide

1. For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.
2. For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.

Configuration Examples The following example binds the IP address 192.168.1.100 on the interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10 binding
192.168.1.100
Ruijie(config)# end
```

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on the interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10 binding
00d0.f800.5555 vlan 1 192.168.1.100
Ruijie(config)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding in interface configuration mode.
switchport port-security mac-address	Sets the static secure address.
switchport port-security aging	Sets the aging time for secure address.

Platform N/A

Description

9.6 switchport port-security interface mac-address

Use this command to configure the static secure address.

Use the **no** form of this command to remove the configuration.

switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]


no switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]

Use this command to configure the static secure address.

Use the **no** form of this command to remove the configuration.

switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]

Parameter Description

Parameter	Description
<i>interface-id</i>	interface ID.
<i>mac-address</i>	Static secure address
<i>vlan-id</i>	VLAN ID of the MAC address
	 The configuration of <i>vlan-id</i> is only supported on the TRUNK port.

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security interface g0/10 mac-address
00d0.f800.5555 vlan 2
Ruijie(config)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
switchport port-security mac-address	Sets the static secure address in interface configuration mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform N/A

Description


9.7 switchport port-security mac-address

Use this command to configure the static secure address.

Use the **no** form of this command to remove the configuration.

switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]

no switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]

Parameter Description	Parameter	Description
	<i>mac-address</i>	Static secure MAC address
	<i>vlan-id</i>	VLAN ID of the MAC address
		 The configuration of <i>vlan-id</i> is only supported on the TRUNK port.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the static secure address and VLAN ID of TRUNK port 10 to

00d0.f800.5555 and 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan
2
Ruijie(config-if)# end
```

Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.
	switchport port-security binding	Configures the secure address binding.
	switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
	switchport port-security aging	Sets the aging time for the secure address.

Platform N/A

Description

9.8 switchport port-security mac-address sticky

Use this command to configure the Sticky MAC secure address.

Use the **no** form of this command to restore the default setting.

switchport port-security mac-address sticky *mac-address* [**vlan** *vlan-id*]

no switchport port-security mac-address sticky *mac-address* [**vlan** *vlan-id*]


Use the command without parameters to enable the Sticky MAC address learning.

Use the **no** form of this command to disable the Sticky MAC address learning.

switchport port-security mac-address sticky

no switchport port-security mac-address sticky

Parameter Description

Parameter	Description
<i>mac-address</i>	Static secure address
<i>vlan-id</i>	Vlan ID of the MAC address
	 The configuration of <i>vlan-id</i> is only supported on the TRUNK port.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Sticky MAC addresses, either static or dynamic, are special addresses free from aging.

Configuration Examples The following example sets the MAC address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 to 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan
2
Ruijie(config-if)# end
```

The following example enables the Sticky MAC address learning on interface g0/10.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security sticky mac-address
Ruijie(config-if)# end
```

Related Commands

Command	Description
---------	-------------

show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
switchport port-security mac-address	Sets the static secure address in interface configuration mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform N/A

Description

9.9 switchport port-security maximum

Use this command to set the maximum number of port secure addresses.

Use the **no** form of this command to restore the default setting.

switchport port-security maximum *value*

no switchport port-security maximum

Parameter Description	Parameter	Description
	<i>value</i>	Maximum number of the secure address, in the range from 1 to 128.

Defaults The default is 128.

Command Mode Interface configuration mode

Usage Guide The number of the secure address contains the sum of static secure address and dynamically learnt secure address, 128 by default.
If the number of the secure address you set is less than current number, it will prompt this setting failure.

Configuration Examples The following example sets the maximum number of the secure address to 2 for interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security maximum 2
Ruijie(config-if)# end
```

Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.

switchport port-security binding	Configures the secure address binding.
Switchport port-security mac-address	Sets the static secure address in the interface configuration mode.
switchport port-security aging	Sets the aging time for the port secure address.

Platform N/A

Description

10 Storm Control Commands

10.1 show storm-control

Use this command to display storm suppression information.

show storm-control [*interface-type interface-number*]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	Specifies an interface.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays storm control configuration on FastEthernet 0/1.

```
Ruijie# show storm-control fastEthernet 0/1
Interface          Broadcast Control Multicast Control Unicast Control
Action
-----
FastEthernet 0/1  1%                50%                1%                none
```

Related Commands	Command	Description
	storm-control	Enables storm suppression.

Platform N/A

Description

10.2 storm-control

Use this command to enable the storm suppression for unknown unicast packets.

Use the **no** or **default** form of this command to restore the default setting.

storm-control unicast [{ *level percent* | **pps packets** | *rate-bps* }]

no storm-control unicast

default storm-control unicast

Use this command to enable the storm suppression for multicast packets.

Use the **no** or **default** form of this command to restore the default setting.

storm-control multicast [{ **level** *percent* | **pps** *packets* | *rate-bps* }]

no storm-control multicast

default storm-control multicast

Use this command to enable the storm suppression for broadcast packets.

Use the **no** or **default** form of this command to restore the default setting.

storm-control broadcast [{ **level** *percent* | **pps** *packets* | *rate-bps* }]

no storm-control broadcast

default storm-control broadcast

Parameter Description	Parameter	Description
	level <i>percent</i>	Sets the bandwidth percentage, for example, 20 means 20%.
	pps <i>packets</i>	Sets the pps, which means packets per second.
	<i>rate-bps</i>	Rate allowed

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms.

A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

Configuration Examples The following example enables the multicast storm suppression on FastEthernet 0/1 and sets the allowed rate to 4M.

```
Ruijie(config)# int fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# storm-control multicast 4096
```

Related Commands	Command	Description
	show storm-control	Displays storm suppression information.

Platform Description N/A

11 SSH Commands

11.1 crypto key generate

Use this command to generate a public key to the SSH server.

crypto key generate { rsa | dsa }


Parameter	Parameter	Description
Description	rsa	Generates an RSA key.
	dsa	Generates a DSA key.


Defaults By default, the SSH server does not generate a public key.

Command Global configuration mode

Mode

Usage Guide When you need to enable the SSH SERVER service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

 Only DSA/RSA authentication is available for one connection. Also, the key algorithm may differ in different client. Thus, it is recommended to generate both RSA and DSA keys so as to ensure connection with the portal server.

 RSA has a minimum modulus of 512 bits and a maximum modulus of 2,048 bits; DSA has a minimum modulus of 360 bits and a maximum modulus of 2,048 bits. For some clients like SCP clients, a 768-bit or more key is required. Thus, it is recommended to generate the key of 768 bits or more.

 A key can be deleted by using the **no crypto key generate** command. The **no crypto key zeroize** command is not available.

Configuration The following example generates an RSA key to the SSH server.

Examples

```
Ruijie# configure terminal
Ruijie(con fig)# crypto key generate rsa
```

Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.
	crypto key zeroize { rsa dsa }	Deletes DSA and RSA keys and disables the SSH server function.

Platform N/A

Description

11.2 crypto key zeroize

Use this command to delete a public key to the SSH server.

crypto key zeroize { rsa | dsa }

Parameter	Parameter	Description
Description	rsa	Deletes the RSA key.
	dsa	Deletes the DSA key.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command deletes the public key to the SSH server. After the key is deleted, the SSH server state becomes DISABLE. If you want to disable the SSH server, run the **no enable service ssh-server** command.

Configuration The following example deletes a RSA key to the SSH server.

Examples

```
Ruijie# configure terminal
Ruijie(config)# crypto key zeroize rsa
```

Related	Command	Description
Commands	show ip ssh	Displays the current status of the SSH server.
	crypto key generate { rsa dsa }	Generates DSA and RSA keys.

Platform N/A

Description

11.3 disconnect ssh

Use this command to disconnect the established SSH connection.

disconnect ssh [vty] session-id

Parameter	Parameter	Description
Description	vtty	Established VTY connection
	<i>session-id</i>	ID of the established SSH connection, in the range from 0 to 35

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

Configuration Examples The following example disconnects the established SSH connection by specifying the SSH session ID.

```
Ruijie# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
Ruijie# disconnect ssh vty 1
```

Related Commands	Command	Description
	show ssh	Displays the information about the established SSH connection.
	clear line vty <i>line_number</i>	Disconnects the current VTY connection.

Platform Description N/A

11.4 disconnect ssh session

Use this command to disconnect the suspended SSH client session.

disconnect ssh-session *session-id*

Parameter Description	Parameter	Description
		<i>session-id</i>

Defaults N/A

Command Mode User EXEC mode

Usage Guide This command is used to disconnect the suspended SSH client session by specifying its session ID.

Configuration Examples The following example disconnects a SSH client session by specifying its session ID.

```
Ruijie# disconnect ssh-session 1
```

Related Commands	Command	Description
		N/A

Platform N/A

Description

11.5 ip scp server enable

Use this command to enable the SCP server function on a network device.

Use the **no** form of this command to restore the default setting.

ip scp server enable

no ip scp server enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.

Configuration The following example enables the SCP server function.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.

Platform N/A

Description

11.6 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter	Parameter	Description
Description	<i>retry times</i>	Authentication retry times, ranging from 0 to 5

Defaults The default is 3.

Command Global configuration mode

Mode

Usage Guide User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to display the configuration of the SSH server

Configuration The following example sets the authentication retry times to 2.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip ssh authentication-retries 2
```

Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.

Platform N/A

Description

11.7 ip ssh cipher-mode

Use this command to set the SSH server encryption mode.

Use the **no** form of this command to restore the default setting.

ip ssh cipher-mode { cbc | ctr | others }

no ip ssh cipher-mode

Parameter	Parameter	Description
Description	cbc	Encryption mode: CBC (Cipher Block Chaining) Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blow fish-CBC
	ctr	Encryption mode: CTR (Counter) Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR
	others	Encryption mode: Others Encryption algorithm: RC4

Defaults All encryption modes are supported by default.

Command Global configuration mode

Mode

Usage Guide This command is used to set the SSH server encryption mode.

For Ruijie Networks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above.

With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and enterprises demanding high security.

Configuration The following example enables CTR encryption mode.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip ssh cipher-mode ctr
```

Platform N/A

Description

11.8 ip ssh hmac-algorithm

Use this command to set the algorithm for message authentication.

Use the **no** form of this command to restore the default setting.

ip ssh hmac-algorithm { md5 | md5-96 | sha1 | sha1-96 }

no ip ssh hmac-algorithm

Parameter	Parameter	Description
Description	md5	MD5 algorithm
	md5-96	MD5-96 algorithm
	sha1	SHA1 algorithm
	sha1-96	SHA1-96 algorithm

Defaults SSHv1: all the algorithms are not supported.

SSHv2: all the algorithms are supported.

Command Global configuration mode

Mode

Usage Guide Ruijie SSHv1 servers do not support algorithms for message authentication.

For Ruijie Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, and SHA1-96 algorithms. Set the algorithm on your demand.

Configuration The following example sets the algorithm for message authentication to SHA1.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip ssh hmac-algorithm sha1
```

Platform N/A

Description

11.9 ip ssh peer

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.

Use the **no** form of this command to restore the default setting.

ip ssh peer *username* **public-key** { *rsa* | *dsa* } *filename*
no ip ssh peer *username* **public-key** { *rsa* | *dsa* } *filename*

Parameter	Parameter	Description
Description	<i>username</i>	User name
	<i>filename</i>	Name of a public key file
	rsa	The public key is a RSA key
	dsa	The public key is a DSA key

Defaults N/A

Command Global configuration mode

Mode

Usage Guide N/A

Configuration The following example sets RSA and DSA key files associated with user **test**.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
Ruijie(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

Related	Command	Description
Commands	show ip ssh	Displays the current status of the SSH server.

Platform N/A

Description

11.10 ip ssh source-interface

Use this command to specify a source interface for the SSH client. Use the **no** form of this command to remove the setting.

ip ssh source-interface *interface-name*
no ip ssh source-interface

Parameter	Parameter	Description
Description	<i>interface-name</i>	Specifies a source interface for the SSH client, indicating that the SSH client takes the interface IP address as its source address.

Defaults The IP address of the interface that sends the SSH packet is taken as its source address by default.

Command Global configuration mode

Mode

Usage Guide This command is used to specify the IP address of the specified interface as the source address of

the SSH client.

Configuration Examples The following example specifies the IP address of interface Loopback 1 as the source address of the global SSH session.

```
Ruijie(config)# ip ssh source-interface Loopback 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

11.11 ip ssh time-out

Use this command to set the authentication timeout for the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh time-out *time*

no ip ssh time-out

Parameter Description	Parameter	Description
	<i>time</i>	Authentication timeout, in the range from 1 to 120 in the unit of seconds

Defaults The default is 120 seconds.

Command Mode Global configuration mode

Usage Guide The authentication is considered timeout and failed if the authentication is not successful within 120 seconds starting from receiving a connection request. Use the **show ip ssh** command to display the configuration of the SSH server.

Configuration Examples The following example sets the timeout value to 100 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip ssh time-out 100
```

Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

11.12 ip ssh version

Use this command to set the version of the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh version { 1 / 2 }

no ip ssh version

Parameter	Parameter	Description
Description	1	Supports the SSH1 client connection request.
	2	Supports the SSH2 client connection request.

Defaults SSH1 and SSH2 are compatible by default.

Command Global configuration mode

Mode

Usage Guide This command is used to configure the SSH connection protocol version supported by SSH server. By default, the SSH server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH server. Use the **show ip ssh** command to display the current status of SSH server.

Configuration The following example sets the version of the SSH server.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip ssh version 2
```

Related	Command	Description
Commands	show ip ssh	Displays the current status of the SSH server.

Platform N/A

Description

11.13 show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

show crypto key mypubkey { rsa | dsa }

Parameter	Parameter	Description
Description	rsa	Displays the RSA key.
	dsa	Displays the DSA key.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode

Usage Guide This command is used to show the information about the public key part of the generated public key on the SSH server, including key generation time, key name, contents in the public key part, etc.

Configuration Examples The following example displays the information about the public key part of the public key to the SSH server.

```
Ruijie(config)#show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
Key name: RSA1 private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:
      AAAAAwEA AQAAAEAA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O
Q10kz+4/
      /IgYR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw==

% Key pair was generated at: 7:1:25 UTC Jan 16 2013
Key name: RSA private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:
      AAAAAwEA AQAAAEAA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi
BbZGZvn3
      LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i8OakQ==
```

Related Commands	Command	Description
	<code>crypto key generate { rsa dsa }</code>	Generates DSA and RSA keys.

Platform Description N/A

11.14 show ip ssh

Use this command to display the information of the SSH server.

show ip ssh


Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Privileged EXEC mode/Global configuration mode

Mode

Usage Guide This command is used to display the information of the SSH server, including version, enablement state, authentication timeout, and authentication retry times.

 If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH version has been configured.

Configuration The following example displays the information of the SSH server.

Examples

```
SSH and SCP disabled:
Ruijie(config)#show ip ssh
SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

SSH and SCP enabled:
Ruijie(config)#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

Related**Commands**

Command	Description
ip ssh version {1 2}	Configures the version for the SSH server.
ip ssh time-out time	Sets the authentication timeout for the SSH server.
ip ssh authentication-retries	Sets the authentication retry times for the SSH server.

Platform N/A

Description

11.15 show ssh

Use this command to display the information about the established SSH connection.

show ssh

Parameter**Description**

Parameter	Description
N/A	N/A

Defaults

N/A

Command

Privileged EXEC mode/Global configuration mode

Mode

Usage Guide This command is used to display the information about the established SSH connection, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.

Configuration The following example displays the information about the established SSH connection:

Examples

```
Ruijie#show ssh
Connection Version Encryption      Hmac      Compress  State
Username
      0      1.5 blowfish                      zlib      Session started test
      1      2.0 aes256-cbc    hmac-sha1  zlib      Session started test
```

Field Description

Field	Description
Connection	VTY number
Version	SSH version
Encryption	Encryption algorithm
Hmac	Message authentication algorithm
Compress	Compress algorithm
State	Connection state
Username	Username

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

11.16 show ssh session

Use this command to display the SSH Client session.

show ssh-session

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode User EXEC mode

Usage Guide Use this command to display the established SSH client session information, including the VTY number, SSH version, encryption algorithm, message authentication algorithm, connection state, and username.

Configuration The following example display the established SSH client session.

```

Examples
Ruijie#show ssh-session
Connect No.  SSH Version  Server Address
-----
0           2.0          192.168.23.122
1           1.5          192.168.23.122
    
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

11.17 ssh

Use this command to establish an encrypted session with a remote device.

```

ssh [ oob ] [ -v { 1 | 2 } ] [ -c { 3des | aes128-cbc | aes192-cbc | aes256-cbc } ] [ -l username ] [ -m { hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 } ] [ -p port-num ] { ip-addr | hostname } [ via mgmt-name ] [ /source { ip A.B.C.D | ipv6 X:X:X:X::X | interface interface-name } ] [ /vrf vrf-name ]
    
```

Parameter Description	Parameter	Description
	oob	Connects to the SSH server through out-of-band communication (generally through MGMT port), This parameter will be displayed only when the device has a MGMT port.
	-v	(Optional) The version of the SSH that is used to connect to the server, By default, it is SSHv2 <ul style="list-style-type: none"> ● Connect to the server via SSHv1. ● Connect to the server via SSHv2.
	-c { 3des aes128-cbc aes192-cbc aes256-cbc }	(Optional) Specifies the encryption algorithm. The available encryption includes Data Encryption Standard (DES), Triple Data Encryption Algorithm (3DES), and Advantaged Encryption Standard (AES). Based on the length of the secret key, AES can be further divided into three types: aes128-cbc (128-bit secret key), aes192-cbc (192-bit secret key), and aes256-cbc (256-bit secret key). If no encryption algorithm is specified, the SSH client will send the supported encryption algorithm list to the server for algorithm negotiation, Otherwise, the SSH client will sent only the specified encryption algorithm to the server, If the server does not support the encryption algorithm, the session will be closed.
	-l <i>username</i>	(Mandatory) The login username.





-m { hmac-md5-96 hmac-md5-128 hmac-sha1-96 hmac-sha1-160 }	(Optional) Specifies a Hash-based message authentication code (HMAC). SSHv1 does not support HMACs. If the user specifies SSHv1 and HMACs at the same time, the HMACs configuration does not take effect. If no algorithm is specified, the SSH client will send the supported HMAC algorithm list to the server for algorithm negotiation, Otherwise, the SSH client will sent only the specified HMAC algorithm to the server, If the server does not support the HMAC algorithm, the session will be closed.
-p <i>port-num</i>	(Optional) Specifies the port number that is used to connect to the SSH server. The port number is 22 by default.
<i>ip-addr</i> <i>hostname</i>	(Mandatory) Specifies the IPv4/IPv6 address or host name for the SSH server,
via <i>mgmt-name</i>	Specifies the MGMT interface for the oob parameter.
/source	Specifies the source IP address or the source interface for the SSH client.
ip A.B.C.D	Specifies the source IPv4 address for the SSH client.
ipv6 X:X:X::X	Specifies the source IPv6 address for the SSH client.
interface <i>interface-name</i>	Specifies the source interface for the SSH client.
/vrf <i>vrf-name</i>	Specifies the VRF routing table to be queried.

Defaults N/A

Command User EXEC mode

Mode

Usage Guide Use the **ssh** command to create a secure and encrypted session between the current device (SSH client) and the other device (SSH server, or the server that supports SSHv1 or SSHv2). This session is similar to the Telnet session except that the SSH session is encrypted. Therefore, the SSH client can create a secure session on the insecure network based on authentication and encryption.

-  SSHv1 supports only DES (56-bit key) and 3DES (168-bit key).
-  SSHv2 supports the following AES algorithm: aes128-cbc, aes192-cbc and aes256-cbc.
-  SSHv1 does not support HMAC algorithm.
-  If the specified SSH version is incompatible with the specified encryption algorithm or authentication algorithm, the algorithm configuration does not take effect.

Configuration Examples The following example creates a session with the username **admin** to the SSH server whose IP address is 192.168.23.122 via SSH.

```
Ruijie#ssh -l admin 192.168.23.122
```

The following example creates a session with the username **admin** to the SSH server whose IP address is 192.168.23.122 via SSHv2, setting aes128-cbc and hmac-md5-128 as encryption

algorithm and authentication algorithm respectively.

```
Ruijie#ssh -v 2 -c aes128-cbc -m hmac-md5-128 -l admin 192.168.23.122
```

Related Commands	Command	Description
	N/A	N/A

11.18 ssh session

Use this command to restore the suspended SSH client session.

ssh-session *session-id*

Parameter	Parameter	Description
Description	<i>session-id</i>	ID of the SSH client session to be restored

Defaults N/A

Command Mode User EXEC mode

Usage Guide After creating the SSH client session via the **SSH** command, you can use the hot key (ctrl+shift+6 x) to temporarily suspend the session, If you want to restore the suspended SSH client session, run the **ssh-session** command. Use the **show ssh-session** command to display the established session.

Configuration Examples The following example restores the suspended SSH client session:

```
Ruijie# ssh-session 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12 URPF Commands

12.1 clear ip urpf

Use this command to clear IPv4 URPF packet drop statistics.

clear ip urpf [**interface** *interface-name*]

Parameter Description	Parameter	Description
	interface <i>interface-name</i>	Clears statistics on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If no interface is specified, IPv4 URPF packet drop statistics on all interfaces are cleared by default.

Configuration Examples The following example clears IPv4 URPF packet drop statistics on port GigabitEthernet 0/1.

```
Ruijie# clear ip urpf interface gigabitEthernet0/1
```

The following example clears IPv4 URPF packet drop statistics on all interfaces.

```
Ruijie# clear ip urpf
```

Related Commands	Command	Description
	show ip urpf	Displays the URPF configuration and statistics.

Platform Description N/A

12.2 ip verify unicast source reachable-via (Interface Configuration Mode)

Use this command to enable the IPv4 URPF feature in the interface configuration mode.

Use the **no** form of this command to restore the default setting.

ip verify unicast source reachable-via { **rx** | **any** } [**allow-default**] [*acl-id*]

no ip verify unicast

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

rx	URPF check in the strict mode. In the strict mode, the egress port for the forwarding entry in the forwarding list found through the source address for the IP packet shall be matched with the ingress port.
any	URPF check in the loose mode. In the loose mode, the forwarding entry for the source address for the IP packet can be found in the forwarding list.
allow-default	(Optional) Allows using the default route to check URPF.
<i>acl-id</i>	(Optional) Sets the ACL number: 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)

Defaults This function is disabled by default.

Command Interface configuration mode

Mode


Usage Guide To determine whether the route for the source address is in the forwarding list or not and the packet validity, enable the URPF feature to check the source address for the received IP packets. If no forwarding entry is matched, the packets are illegal.

Enabling URPF feature in the interface configuration mode enables URPF check for the received packets on the interface.

By default, the default route is not used for URPF check. Use the keyword `allow-default` to enable the URPF check.

By default, the packets that failed to pass the URPF check are dropped. With ACL (`acl-name`) configured, the ACL matching continues when the routing fails. The packets will be dropped if the ACL is inexistent or the deny ACE is matched; otherwise, if the permit ACE is matched, the packets will be forwarded.

 After this command is used, URPF check on IPv4 packets will be enabled.

 This function is supported only on routed and Layer 3 interfaces, and have the following restrictions:

- Not support the ACL association;
Not support to use the IPv6 route with prefix in 65 to 127 bits for the URPF check;
- After enabling the URPF feature, the range of packets received on the interface will be expanded, that is, the URPF feature is enabled for all packets received on the physical ports.
- After enabling the URPF feature, it halves the route forwarding capacity.
- After enabling the URPF feature in the strict mode, the user can match the equivalent route when URPF check is enabled for the packets received on the interface.

 URPF feature cannot be configured in the global configuration mode and in the interface configuration mode at the same time.

Configuration The following example checks the URPF feature of the received packets in the strict mode on the interface GigabitEthernet 0/1.

Examples

```
Ruijie(config)# interface gigabitEthernet0/1
Ruijie(config-if-GigabitEthernet 0/1) # ip verify unicast source reachable-via rx
```

Related Commands

Command	Description
show ip urpf	Displays the URPF information.

Platform N/A

Description

12.3 ip verify urpf drop-rate compute interval

Use this command to set the URPF drop-rate compute interval.

Use the **no** form of this command to restore the default setting.

ip verify urpf drop-rate compute interval *seconds*

no ip verify urpf drop-rate compute interval

Parameter Description

Parameter	Description
<i>seconds</i>	Sets the URPF drop-rate compute interval, in the range from 30 to 300 in the unit of seconds.

Defaults The default is 30 seconds.

Command Mode Global configuration mode

Usage Guide The URPF drop-rate is computed globally for both IPv4 and IPv6 packets on interfaces enabled with URPF.

Configuration The following example sets the URPF drop-rate compute interval as 60 seconds.

Examples

```
Ruijie(config)# ip verify urpf drop-rate compute interval 60
```

Related Commands

Command	Description
ip verify urpf drop-rate notify	Sets the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
ip verify urpf notification threshold	Sets the URPF drop-rate threshold.

Platform N/A

Description

12.4 ip verify urpf drop-rate notify

Use this command to enable the URPF drop-rate monitoring.

Use the **no** or **default** form of this command to restore the default setting.

ip verify urpf drop-rate notify

no ip verify urpf drop-rate notify

default ip verify urpf drop-rate notify

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide This command is used to enable the URPF drop-rate monitoring, notifying the user of the URPF packet drop information by means of Syslog or Trap for the convenience of the user network monitoring.

Configuration The following example enables the URPF drop-rate monitoring on port GigabitEthernet 0/1.

Examples

```
Ruijie(config)# interface gigabitEthernet0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
```

Related Commands	Command	Description
	ip verify urpf drop-rate compute interval	Sets the URPF drop-rate compute interval.
	ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
	ip verify urpf notification threshold	Sets the URPF drop-rate threshold.

Platform N/A

Description

12.5 ip verify urpf drop-rate notify hold-down

Use this command to set the URPF drop-rate notification interval.

Use the **no** form of this command to restore to the default setting.

ip verify urpf drop-rate notify hold-down *seconds*

no ip verify urpf drop-rate notify hold-down

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the URPF drop-rate notification interval, in the range from 30 to 300 in the unit of seconds.

Defaults The default is 300 seconds.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the URPF drop-rate notification interval as 60 seconds.

```
Ruijie(config)# ip verify urpf drop-rate notify hold-down 60
```

Related Commands	Command	Description
	ip verify urpf drop-rate compute interval	Sets the URPF drop-rate computing interval.
	ip verify urpf drop-rate notify	Sets the URPF drop-rate monitoring.
	ip verify urpf notification threshold	Sets the URPF drop-rate threshold.

Platform Description N/A

12.6 ip verify urpf notification threshold

Use this command to set the URPF drop-rate threshold.

Use the **no** form of this command to restore the default setting.

ip verify urpf notification threshold *rate-value*

no ip verify urpf notification threshold

Parameter Description	Parameter	Description
	threshold <i>rate-value</i>	Sets the URPF drop-rate threshold, in the range from 0 to 4294967295 in the unit of packets per second (pps).

Defaults The default is 1,000 pps.

Command Mode Interface configuration mode

Usage Guide The threshold 0 indicates that once the device detects a dropped packet due to the IPv4 URPF check, the notification is sent.
The user can adjust the drop-rate threshold value according to the actual network performance.

Configuration The following example sets the URPF drop-rate threshold 10pps on the interface GigabitEthernet 0/1.

Examples

```
Ruijie(config)# interface gigabitEthernet0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 verify urpf drop-rate notify
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 verify urpf notification
threshold 10
```

**Related
Commands**

Command	Description
ip verify urpf drop-rate compute interval	Sets the URPF drop-rate computing interval.
ip verify urpf drop-rate notify	Sets the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate notification interval.

Platform N/A

Description

12.7 show ip urpf

Use this command to display the IPv4 URPF configuration and statistics.

show ip urpf [interface *interface-name*]

**Parameter
Description**

Parameter	Description
interface <i>interface-name</i>	Displays the configuration and statistics on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide The global configuration and statistics of all interfaces are displayed by default.

Configuration The following example displays IPv4 URPF configuration and statistics on port GigabitEthernet 0/1.

Examples

```
Ruijie# show ip urpf interface gigabitEthernet0/21
IP verify source reachable-via RX
IP verify URPF drop-rate notify disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 0
```

Field	Description
IP verify source reachable-via xx	xx in strict mode is displayed as RX and in loose mode as ANY.

IP verify URPF drop-rate notify xx	If drop rate notification is enabled, xx is displayed as enabled. Otherwise, it is displayed as disabled.
IP verify URPF notification threshold is xxpps	The threshold of URPF drop rate, in the range from 0 to 4294967295 in the unit of packets per second (pps). The default is 1000.
Number of drop packets in this interface is x	The number of drop packets
Number of drop-rate notification counts in this interface is x	The URPF drop-rate notification counts

The following example displays IPv4 URPF configuration and statistics.

```
Ruijie# show ip urpf
IP verify URPF drop-rate compute interval is 30s
IP verify URPF drop-rate notify hold-down is 300s

Interface GigabitEthernet 0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 2
```

Field	Description
IP verify URPF drop-rate compute interval is x	Drop-rate computing interval
IP verify URPF drop-rate notify hold-down is x	Drop-rate notification interval
Interface interface-name	interface-name is the name of the interface on which URPF is applied. Configuration and statistics on this interface are displayed.

Related Commands

Command	Description
ip verify unicast source reachable-via	Enables the URPF features.
ip verify urpf drop-rate compute interval	Sets the URPF drop-rate compute interval.
ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
ip verify urpf notification threshold	Sets the URPF drop-rate threshold.
clear ip urpf	Clears the URPF statistical information.

Platform Description

N/A

13 CPU Protection Commands

13.1 clear cpu-protect-counters

Use this command to clear the CPP statistics.

clear cpu-protect counters [**device** *device_num*] [**slot** *slot_num*]

Parameter Description	Parameter	Description
	<i>device_num</i>	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.
	<i>slot_num</i>	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears the CPP statistics.

```

Examples
Ruijie(config)#show cpu-protect type bpdu
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total
Drop  Total HW_Drop
-----
-----
bpdu              6              200              0           0           600    50
50
Ruijie#clear cpu-protect counters
Ruijie(config)#show cpu-protect type bpdu
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total
Drop  Total HW_Drop
-----
-----
bpdu              6              200              0           0           0      0

```

0

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

13.2 clear cpu-protect-counters mboard

Use this command to clear the CPP statistics on the supervisor module.

clear cpu-protect counters mboard

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears the CPP statistics on the supervisor module.

```

Examples
Ruijie(config)#show cpu-protect type bpdu
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total
Drop Total HW_Drop
-----
-----
-----
bpdu              6              200              0           0           600     50
50
Ruijie#clear cpu-protect counters mboard
Ruijie(config)#show cpu-protect type bpdu
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total
Drop Total HW_Drop
-----
-----
-----
bpdu              6              200              0           0           0        0
0
    
```

Related Commands	Command	Description

N/A	N/A
-----	-----

Platform N/A
Description

13.3 cpu-protect cpu bandwidth

Use this command to configure the bandwidth for the CPU port. Use the **no** form of this command to restore the default setting.

cpu-protect cpu bandwidth *bandwidth_value*
no cpu-protect cpu bandwidth

Parameter Description	Parameter	Description
	<i>bandwidth_value</i>	An integer number ranges from 0 to 100,000 (PPS). Indicates the bandwidth value of the CPU port.

Defaults The default CPU port bandwidth varies with products.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the CPU port bandwidth to 32,000pps.

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect cpu bandwidth 32000
Ruijie#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

13.4 cpu-protect traffic-class bandwidth

Use this command to configure the bandwidth for each priority queue. Use the **no** form of this command to restore the default setting.

cpu-protect traffic-class *traffic-class-num* **bandwidth** *bandwidth_value*
no cpu-protect traffic-class *traffic-class-num* **bandwidth**

Parameter Description	Parameter	Description
	<i>traffic-class-num</i>	A default integer that varies with products, indicating the queue priority
	<i>bandwidth_value</i>	An integer number ranges from 0 to 100,000 (pps). Indicates the bandwidth value of the CPU port.

Defaults The default bandwidth of each priority queue varies with products.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example s sets the priority queue 5 to 3500 pps.

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect traffic-class 5 bandwidth 3500
Ruijie#show cpu-protect traffic-class 5
Traffic-class  Bandwidth(pps)  Rate(pps)      Drop(pps)
-----
5              3500              0              0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13.5 cpu-proctect type packet-type bandwidth

Use this command to configure the bandwidth of a specific packet.

Use the **no** form of this command to restore the default setting.

cpu-protect type *packet-type* **bandwidth** *bandwidth_value*

no cpu-protect type *packet-type* **bandwidth**

Parameter Description	Parameter	Description
	<i>packet-type</i>	Packet type, which varies with products
	<i>bandwidth_value</i>	An integer number ranges from 0 to 32,000 (pps). Indicates the bandwidth value of the CPU port.

Defaults The default CPU port bandwidth varies with products.

Command Global configuration mode
Mode

Usage Guide N/A

Configuration The following example sets the BPDU bandwidth to 200 pps.

```

Examples
Ruijie# configure terminal
Ruijie(config)# cpu-protect type bpdu bandwidth 200
Ruijie(config)#show cpu-protect type bpdu
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total      Total Drop
-----
-----
bpdu              6              200              0           0           0           0
    
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

13.6 cpu-protect type traffic-class

Use this command to set the priority queue (PQ) of the packet.
 Use the **no** form of this command to restore the default setting.
cpu-protect type *packet-type* traffic-class *traffic-class-num*
no cpu-protect type *packet-type* traffic-class

Parameter Description	Parameter	Description
	<i>packet-type</i>	
<i>traffic-class-num</i>		An integer number varying with products. Indicates the bandwidth value of the CPU port.

Defaults The default PQ varies with products.

Command Global configuration mode
Mode

Usage Guide N/A

Configuration The following example sets the PQ of BPDU packets to 5.

Examples

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect type bpdu traffic-class 5
Ruijie(config)#show cpu-protect type bpdu
Packet Type          Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total
Drop Total HW_Drop
-----
-----
bpdu                 5              200              0           0           0       0
0
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

13.7 show cpu-protect

Use this command to display all CPP configuration and statistics.

show cpu-protect [**device** *device_num*] [**slot** *slot_num*]

Parameter Description

Parameter	Description
<i>device_num</i>	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.
<i>slot_num</i>	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A

Command Mode All configuraiton mode

Usage Guide N/A

Configuration Examples N/A

Related Commands	Command	Description
		N/A

Platform N/A
Description

13.8 show cpu-protect cpu

Use this command to display the configurations of the CPU port.

show cpu-protect cpu

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples The following example displays the configuration of the CPU port.

```
Ruijie#show cpu-protect cpu
%cpu port bandwidth: 32000 (pps)
```

Related Commands	Command	Description
		N/A

Platform N/A
Description

13.9 show cpu-protect mboard

Use this command to display the statistics of various packets of CPU protection on the management board.

show cpu-protect mboard

Parameter Description	Parameter	Description

N/A	N/A
-----	-----

Defaults N/A

Command Mode All configuration modes

Usage Guide This command displays the statistics of the packets received by CPU on the management board.

Configuration Examples The following example displays the CPP configuration and statistics of the master device.

```
Ruijie#show cpu-protect mboard
%cpu port bandwidth: 80000(pps)
Traffic-class   Bandwidth(pps)  Rate(pps)      Drop(pps)
-----
0               8000            0              0
1               8000            0              0
2               8000            0              0
3               8000            0              0
4               8000            0              0
5               8000            0              0
6               8000            0              0
7               8000            0              0

Packet Type      Traffic-class   Bandwidth(pps)  Rate(pps)      Drop(pps)      Total          Total
Drop Total HW_Drop
-----
bpdu             6              128             0              0              0              0
0
arp              3              10000           0              0              0              0
0
arp-dai          3              10000           0              0              0              0
0
arp-proxy        3              10000           0              0              0              0
0
tpp              7              128             0              0              0              0
0
dot1x            4              128             0              0              0              0
0
gvrp             5              128             0              0              0              0
0
rldp             6              128             0              0              0              0
0
lacp            6              128             0              0              0              0
0
```

rerp	6	128	0	0	0	0
0						
reup	6	128	0	0	0	0
0						
lldp	5	128	0	0	0	0
0						
cdp	5	128	0	0	0	0
0						
dhcps	4	128	0	0	0	0
0						
dhcps6	4	128	0	0	0	0
0						
dhcp6-client	4	128	0	0	0	0
0						
dhcp6-server	4	128	0	0	0	0
0						
dhcp-relay-c	4	128	0	0	0	0
0						
dhcp-relay-s	4	128	0	0	0	0
0						
option82	4	128	0	0	0	0
0						
tunnel-bpdu	5	128	0	0	0	0
0						
tunnel-gvrp	5	128	0	0	0	0
0						
unknown-v6mc	3	128	0	0	0	0
0						
known-v6mc	3	128	0	0	0	0
0						
xgv6-ipmc	3	128	0	0	0	0
0						
stargv6-ipmc	3	128	0	0	0	0
0						
unknown-v4mc	3	128	0	0	0	0
0						
known-v4mc	3	128	0	0	0	0
0						
xgv-ipmc	3	128	0	0	0	0
0						
sgv-ipmc	3	128	0	0	0	0
0						
udp-helper	4	128	0	0	0	0
0						

dvmrp	5	128	0	0	0	0
0						
igmp	4	128	0	0	0	0
0						
icmp	4	128	0	0	0	0
0						
ospf	5	128	0	0	0	0
0						
ospf3	5	128	0	0	0	0
0						
pim	6	128	0	0	0	0
0						
pimv6	6	128	0	0	0	0
0						
rip	6	128	0	0	0	0
0						
ripng	6	128	0	0	0	0
0						
vrrp	6	128	0	0	0	0
0						
vrrp6	6	128	0	0	0	0
0						
ttl0	6	128	0	0	0	0
0						
ttl1	6	128	0	0	0	0
0						
err_hop_limit	1	800	0	0	0	0
0						
local-ipv4	6	128	0	0	0	0
0						
local-ipv6	6	128	0	0	0	0
0						
route-host-v4	0	4096	0	0	0	0
0						
route-host-v6	0	4096	0	0	0	0
0						
mld	0	1000	0	0	0	0
0						
nd-snp-ns-na	6	128	0	0	0	0
0						
nd-snp-rs	6	128	0	0	0	0
0						
nd-snp-ra-redirect	6	128	0	0	0	0
0						

nd-non-snp 0	6	128	0	0	0	0
erps 0	4	128	0	0	0	0
mpls-ttl0 0	6	128	0	0	0	0
mpls-ttl1 0	6	128	0	0	0	0
mpls-ctrl 0	6	128	0	0	0	0
isis 0	5	2000	0	0	0	0
bgp 0	1	128	0	0	0	0
cfm 0	0	128	0	0	0	0
fcoe-fip 0	6	128	0	0	0	0
fcoe-local 0	6	128	0	0	0	0
bfd-echo 0	6	5120	0	0	0	0
bfd-ctrl 0	6	5120	0	0	0	0
madp 0	7	1000	0	0	0	0
ip4-other 0	6	128	0	0	0	0
ip6-other 0	6	128	0	0	0	0
non-ip-other 0	6	20000	0	0	0	0
trill 0	2	1000	0	0	0	0
trill-oam 0	2	1000	0	0	0	0
efm 0	2	1000	0	0	0	0

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

13.10 show cpu-protect summary

Use this command to display the CPP configuration and statistics of the master device.

show cpu-protect summary

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples

```
Ruijie#show cpu-protect summary
%cpu port bandwidth: 80000(pps)
Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
-----
0              8000              0           0
1              8000              0           0
2              8000              0           0
3              8000              0           0
4              8000              0           0
5              8000              0           0
6              8000              0           0
7              8000              0           0

Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total
Drop  HW Total  HW Total Drop
-----
bpdu              6              128             0           0           0       0
0  0
arp               3             10000           0           0           0       0
0  0
arp-dai           3             10000           0           0           0       0
0  0
arp-proxy         3             10000           0           0           0       0
0  0
tpp               7              128             0           0           0       0
0  0
```

dot1x	4	128	0	0	0	0
0 0						
gvrp	5	128	0	0	0	0
0 0						
rldp	6	128	0	0	0	0
0 0						
lacp	6	128	0	0	0	0
0 0						
rerp	6	128	0	0	0	0
0 0						
reup	6	128	0	0	0	0
0 0						
lldp	5	128	0	0	0	0
0 0						
cdp	5	128	0	0	0	0
0 0						
dhcps	4	128	0	0	0	0
0 0						
dhcps6	4	128	0	0	0	0
0 0						
dhcp6-client	4	128	0	0	0	0
0 0						
dhcp6-server	4	128	0	0	0	0
0 0						
dhcp-relay-c	4	128	0	0	0	0
0 0						
dhcp-relay-s	4	128	0	0	0	0
0 0						
option82	4	128	0	0	0	0
0 0						
tunnel-bpdu	5	128	0	0	0	0
0 0						
tunnel-gvrp	5	128	0	0	0	0
0 0						
unknown-v6mc	3	128	0	0	0	0
0 0						
known-v6mc	3	128	0	0	0	0
0 0						
xgv6-ipmc	3	128	0	0	0	0
0 0						
stargv6-ipmc	3	128	0	0	0	0
0 0						
unknown-v4mc	3	128	0	0	0	0
0 0						

known-v4mc 0 0	3	128	0	0	0	0
xgv-ipmc 0 0	3	128	0	0	0	0
sgv-ipmc 0 0	3	128	0	0	0	0
udp-helper 0 0	4	128	0	0	0	0
dvmrp 0 0	5	128	0	0	0	0
igmp 0 0	4	128	0	0	0	0
icmp 0 0	4	128	0	0	0	0
ospf 0 0	5	128	0	0	0	0
ospf3 0 0	5	128	0	0	0	0
pim 0 0	6	128	0	0	0	0
pimv6 0 0	6	128	0	0	0	0
rip 0 0	6	128	0	0	0	0
ripng 0 0	6	128	0	0	0	0
vrrp 0 0	6	128	0	0	0	0
vrrp6 0 0	6	128	0	0	0	0
ttl0 0 0	6	128	0	0	0	0
ttl1 0 0	6	128	0	0	0	0
err_hop_limit 0 0	1	800	0	0	0	0
local-ipv4 0 0	6	128	0	0	0	0
local-ipv6 0 0	6	128	0	0	0	0
route-host-v4 0 0	0	4096	0	0	0	0
route-host-v6 0 0	0	4096	0	0	0	0

mld	0	1000	0	0	0	0
0 0						
nd-snp-ns-na	6	128	0	0	0	0
0 0						
nd-snp-rs	6	128	0	0	0	0
0 0						
nd-snp-ra-redirect	6	128	0	0	0	0
0 0						
nd-non-snp	6	128	0	0	0	0
0 0						
erps	4	128	0	0	0	0
0 0						
mpls-ttl0	6	128	0	0	0	0
0 0						
mpls-ttl1	6	128	0	0	0	0
0 0						
mpls-ctrl	6	128	0	0	0	0
0 0						
isis	5	2000	0	0	0	0
0 0						
bgp	1	128	0	0	0	0
0 0						
cfm	0	128	0	0	0	0
0 0						
fcoe-fip	6	128	0	0	0	0
0 0						
fcoe-local	6	128	0	0	0	0
0 0						
bfd-echo	6	5120	0	0	0	0
0 0						
bfd-ctrl	6	5120	0	0	0	0
0 0						
madp	7	1000	0	0	0	0
0 0						
ip4-other	6	128	0	0	0	0
0 0						
ip6-other	6	128	0	0	0	0
0 0						
non-ip-other	6	20000	0	0	0	0
0 0						
trill	2	1000	0	0	0	0
0 0						
trill-oam	2	1000	0	0	0	0
0 0						

e fm	2	1000	0	0	0	0
0 0						

Related Commands

Command	Description
N/A	N/A

Platform N/A**Description**

13.11 show cpu-protect traffic-class

Use this command to display the summarized configuration and statistics of priority queues.

show cpu-protect traffic-class {*traffic-class-num* | **all**} [**device** *device_num*] [**slot** *slot_num*]

Parameter Description

Parameter	Description
<i>traffic-class-num</i>	A default integer that varies with products, indicating the queue priority.
<i>all</i>	Displays configurations and statistics of all priority queues.
<i>device_num</i>	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.
<i>slot_num</i>	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A**Command Mode** All configuration modes**Usage Guide** N/A**Configuration Examples** The following example displays the summarized configuration and statistics of priority queues.

```
Ruijie#show cpu-protect traffic-class all
Traffic-class  Bandwidth (pps)  Rate (pps)  Drop (pps)
-----
0              8000            0           0
1              8000            0           0
```

2	8000	0	0
3	8000	0	0
4	8000	0	0
5	3200	0	0
6	8000	0	0
7	8000	0	0

Related Commands

Command	Description
N/A	N/A

Platform N/A**Description**

13.12 show cpu-protect type

Use this command to display the statistics of the specified type of packets

show cpu-protect type *packet-type* [**device** *device_num*] [**slot** *slot_num*]

Parameter Description

Parameter	Description
<i>packt-type</i>	Packet type, which varies with products
<i>all</i>	Displays the configurations and statistics of all packet types.
<i>device_num</i>	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.
<i>slot_num</i>	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A**Command** All configuration modes**Mode****Usage Guide** N/A**Configuration** The following example displays the statistics of the ICMP packets.**Examples**

```
Ruijie(config)#show cpu-protect type icmp
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total
```

Drop Total		HW_Drop			
-----		-----		-----	
-----		-----		-----	
icmp	5	1500	50	0	10000
100	100				

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14 DHCP Snooping Commands

14.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP Snooping binding database.


clear ip dhcp snooping binding [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the user MAC address to be cleared.
	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.
	<i>ip</i>	Specifies the IP address to be cleared.
	<i>interface-id</i>	Specifies the ID of the interface to be cleared.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the current dynamic user information from the DHCP Snooping binding database.

 After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.

Configuration Examples The following example clears the dynamic database information from the DHCP Snooping binding database.

```
Ruijie# clear ip dhcp snooping binding
Ruijie# show ip dhcp snooping binding
Total number of bindings: 0
MACAddress IPAddress Lease(sec) Type VLAN Interface
-----
```

Related Commands	Command	Description
	show ip dhcp snooping binding	Displays the information of the DHCP Snooping binding database.

Platform Description N/A

14.2 ip dhcp snooping

Use this command to enable the DHCP Snooping function globally.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping

no ip dhcp snooping

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The **show ip dhcp snooping** command is used to display whether the DHCP Snooping function is enabled.

Configuration The following example enables the DHCP Snooping function.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
```

Related Commands	Command	Description
	show ip dhcp snooping	Displays the configuration information of DHCP Snooping.
	ip dhcp snooping vlan	Configures DHCP Snooping enabled VLAN.

Platform Description N/A

14.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP Snooping BOOTP-bind function.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping bootp-bind

no ip dhcp snooping bootp-bind

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

Configuration Examples The following example enables the DHCP Snooping BOOTP-bind function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping bootp-bind
Ruijie(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

14.4 ip dhcp snooping check-giaddr

Use this command to enable DHCP Snooping to support the function of processing Relay requests. Use the **no** form of this command to restore the default setting.

ip dhcp snooping check-giaddr
no ip dhcp snooping check-giaddr

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet.

After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

Configuration The following example enables DHCP Snooping to support the function of processing Relay requests.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping check-giaddr
Ruijie(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform N/A

Description

14.5 ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP Snooping binding database into the flash periodically.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping database write-delay *time*

no ip dhcp snooping database write-delay

Parameter Description

Parameter	Description
<i>time</i>	The interval at which the system writes the dynamic user information of the DHCP Snooping database into the flash, in the range from 600 to 86,400 in the unit of seconds

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function writes user information into flash in case of loss after restart. In that case, users need to obtain IP addresses again for normal communication.

 Too fast writing will reduce flash durability.

Configuration Examples The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
```



```
Ruijie(config)# end
```

**Related
Commands**

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform N/A**Description**

14.6 ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

ip dhcp snooping database write-to-flash

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A**Command
Mode** Global configuration mode**Usage Guide** This command is used to write the dynamic user information of the DHCP binding database into flash in real time.**Configuration** The following example writes the dynamic user information of the DHCP binding database into flash.**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A**Description**

14.7 ip dhcp snooping information option

Use this command to add option82 to the DHCP request message.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option [standard-format]

no ip dhcp snooping information option [standard-format]


Parameter Description	Parameter	Description
	standard-format	The option82 uses the standard format.

Defaults This function is disabled by default,

Command Mode Global configuration mode

Usage Guide This command adds option82 to the DHCP request messages based on which the DHCP server assigns IP addresses.

By default, this function is in extended mode.

 DHCP Relay function adds option82 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option82 and DHCP Relay at the same time.

Configuration The following example adds option82 to the DHCP request message.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
```

Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

14.8 ip dhcp snooping information option format remote-id

Use this command to set the option82 sub-option remote-id as the customized character string.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option format remote-id { string *ascii-string* | hostname }

no ip dhcp snooping information option format remote-id { string *ascii-string* | hostname }

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
string <i>ascii-string</i>	The content of the option82 remote-id extension format is customized character string.
hostname	The content of the option82 remote-id extension format hostname

Defaults This function is disabled by default.

Command Global configuration mode

Mode

Usage Guide This command sets the remote-id in the option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the option82 information.

Configuration Examples The following example adds the option82 into the DHCP request packets with the content of remote-id as hostname.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option format remote-id hostname
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

14.9 ip dhcp snooping suppression

Use this command to set the port to be the suppression status.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping suppression

no ip dhcp snooping suppression

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP.

This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

Configuration The following example sets **fastEthernet 0/2** to be in the suppression status.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# ip dhcp snooping suppression
Ruijie(config-if)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform N/A

Description

14.10 ip dhcp snooping trust

Use this command to set the trusted ports for DHCP Snooping.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping trust

no ip dhcp snooping trust

Parameter Description

Parameter	Description
N/A	N/A

Defaults All ports are untrusted by default.

Command Interface configuration mode

Mode

Usage Guide Use this command to set a port as a trusted port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded. This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

Configuration The following example sets fastEthernet 0/1 as a trusted port:

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)# end
```

Related

Command	Description
---------	-------------

Commands	
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform N/A

Description

14.11 ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to check the source MAC address of the DHCP request message. If the MAC address in the link-layer header is different from the CHADDR (Client MAC Address), the check fails ,and the packets will be discarded.

Configuration Examples The following example enables the check of the source MAC address of the DHCP request message.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
```

Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform N/A

Description

14.12 ip dhcp snooping vlan

Use this command to enable DHCP Snooping for the specific VLAN.

Use the **no** form of this command to restore the default setting.

```
ip dhcp snooping vlan {vlan-rng | { vlan-min [ vlan-max ] }}
no ip dhcp snooping vlan {vlan-rng | { vlan-min [ vlan-max ] }}
```

Parameter Description	Parameter	Description
	<i>vlan-rng</i>	VLAN range of effective DHCP Snooping
	<i>vlan-min</i>	Minimum VLAN of effective DHCP Snooping
	<i>vlan-max</i>	Maximum VLAN of effective DHCP Snooping

Defaults By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

Command Mode Global configuration mode

Usage Guide Use this command to enable DHCP Snooping for specified VLANs globally.

Configuration Examples The following example enables the DHCP Snooping function in VLAN 1000.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

Related Commands	Command	Description
	ip dhcp snooping	Enables DHCP Snooping globally.

Platform Description N/A

14.13 ip dhcp snooping vlan max-user

Use this command to set the maximum number of users bound with the VLAN.

Use the **no** form of this command to restore the default setting.

```
ip dhcp snooping vlan vlan-word max-user user-number
```

```
no ip dhcp snooping vlan vlan-word max-user user-number
```

Parameter Description	Parameter	Description
	<i>vlan-word</i>	The VLAN range
	<i>user-number</i>	The maximum number of users bound with the VLAN

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to set the maximum number of users bound with the VLAN. This function combined with the corresponding topology can prevent illegal DHCP packet attacks.

Configuration The following example sets the maximum number of users bound with VLAN 1 to 10 and VLAN 20 to 30 respectively.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user
30
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

14.14 ip dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the option82 sub-option circuit-id and change the VLAN in the circuit-id into the specified VLAN.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

no ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

**Parameter
Description**

Parameter	Description
<i>vlan-id</i>	The ID of the VLAN to be replaced

Defaults This function is disabled by default.

**Command
Mode** Interface configuration mode

Usage Guide With this command configured, the option82 is added to the DHCP request packets, the circuit-id in the option82 information is the specified VLAN and the DHCP server will assign the addresses according to the option82 information.

**Configuration
Examples** The following adds the option82 to the DHCP request packets and changes the VLAN 4094 in the option82 sub-option circuit-id to VLAN93:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping vlan 4094 information option
change-vlan-to vlan 4093
Ruijie(config-if)# end
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

14.15 ip dhcp snooping vlan information option format-type circuit-id string

Use this command to configure the option82 sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

no ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

Parameter Description	Parameter	Description
	<i>vlan-id</i>	
<i>ascii-string</i>		The user-defined content to fill to the Circuit ID

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to add the option82 to the DHCP request packets. The content of the sub-option circuit-id is customized with 3 to 63 bytes, and the DHCP server will assign the addresses according the option82 information.

Configuration Examples The following example adds the option82 to the DHCP request packets with the content of the sub-option circuit-id as *port-name*.

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping vlan 4094 information option format-type
circuit-id string port-name
Ruijie(config-if)# end
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

14.16 renew ip dhcp snooping database

Use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.


renew ip dhcp snooping database

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to import the flash file information to the DHCP Snooping database in real time.

 Records out of lease time and repeated will be neglected.

Configuration The following example imports the flash file information to the DHCP Snooping database.

Examples Ruijie# renew ip dhcp snooping database

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

14.17 show ip dhcp snooping

Use this command to display the DHCP Snooping configuration.

show ip dhcp snooping

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the DHCP Snooping configuration.

Examples

```
Ruijie# show ip dhcp snooping
Switch DHCP snooping status :ENABLE
Verification of hwaddr field status :DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                                     Trusted                                     Rate
limit(pps)
-----
-----
GigabitEthernet 0/4                          YES                                     unlimited
Default                                       No
```

**Related
Commands**

Command	Description
ip dhcp snooping	Enables the DHCP Snooping globally.
ip dhcp snooping verify mac-address	Enables the check of source MAC address of DHCP Snooping packets.
ip dhcp snooping write-delay	Sets the interval of writing user information to FLASH periodically.
ip dhcp snooping information option	Adds option82 to the DHCP request message.
ip dhcp snooping bootp-bind	Enables the DHCP Snooping bootp bind function.
ip dhcp snooping trust	Sets the port as a trust port.

Platform N/A

Description

14.18 show ip dhcp snooping binding

Use this command to display the information of the DHCP Snooping binding database.

show ip dhcp snooping binding

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display all the information of the DHCP Snooping binding database.

Configuration Examples 1: The following example displays the information of the DHCP Snooping binding database.

```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
NO.    MACADDRESS          IPADDRESS      LEASE (SEC)   TYPE          VLAN
INTERFACE
-----
-----
1      0000.0000.0001      1.1.1.1       78128         DHCP-Snooping 1
GigabitEthernet 0/1
```

Parameter	Description
Total number of bindings	The total number of bindings in the DHCP Snooping database.
NO.	The record order.
MacAddress	The MAC address of the user.
IpAddress	The IP address of the user.
Lease(sec)	The lease time of the record.
Type	The record type.
VLAN	The VLAN where the user belongs.
Interface	The user's connection interface. It can be a either a wired access interface.

Related Commands	Command	Description
	ip dhcp snooping binding	Adds the static user information to the DHCP Snooping database.
	clear ip dhcp snooping binding	Clears the dynamic user information from the DHCP Snooping binding database.

Platform Description N/A

15 ARP-Check Commands

15.1 arp-check

Use this command to enable the ARP check function on the Layer 2 interface.

Use the **no** form of this command to restore the default setting.

arp-check

no arp-check

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command mode Interface configuration mode

Usage Guide The ARP check function generates the ARP filtering information according to legal user information, implementing the illegal ARP packet filtering on the network.

Configuration Examples This following example enables the APR check function on interface GigabitEthernet 0/1.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# arp-check
Ruijie(config-if-GigabitEthernet 0/1)# end
```

Related Commands	Command	Description
	show interfaces arp-check list	Displays the ARP check entries.

Platform Description N/A

15.2 show interfaces arp-check list

Use this command to display the ARP check entries on the Layer 2 interface.

show { interface [interface-type interface-number] } arp-check list

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>interface-type</i>	Wired interface type
<i>interface-number</i>	Wired interface number

Command mode Privileged EXEC mode

Usage Guide Use this command to display the ARP check entries.

Configuration The following example displays the ARP check entries.

Examples

```
Ruijie(config)#show interfaces arp-check list
```

INTERFACE	SENDER MAC	SENDER IP	POLICY SOURCE
GigabitEthernet 0/1	00D0.F800.0003	192.168.1.3	address-bind
GigabitEthernet 0/1	00D0.F800.0001	192.168.1.1	port-security
GigabitEthernet 0/4		192.168.1.3	port-security
GigabitEthernet 0/5	00D0.F800.0003	192.168.1.3	address-bind
GigabitEthernet 0/7	00D0.F800.0006	192.168.1.6	AAA ip-auth-mode
GigabitEthernet 0/8	00D0.F800.0007	192.168.1.7	GSN

Field	Description
INTERFACE	Interface name
SENDER MAC	Source MAC address
SENDER IP	Source IP address
POLICY SOURCE	Source of the entry

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

16 DAI Commands

16.1 ip arp inspection trust

Use this command to configure the L2 port to a trusted port.

Use the **no** form of this command to restore the L2 port to an untrusted port.

ip arp inspection trust

no ip arp inspection trust

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The L2 port is untrusted.

Command Mode Interface configuration mode

Usage Guide If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.

Configuration Examples The following example sets the gigabitEthernet 0/19 interface as the trusted port.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/19
Ruijie(config-if-GigabitEthernet 0/19)# ip arp inspection trust
Ruijie(config-if-GigabitEthernet 0/19)# end
```

Related Commands	Command	Description
	show ip arp inspection interface	Displays related DAI information on the interface, including the trust state and rate limit of the interface.

Platform Description N/A

16.2 ip arp inspection vlan

Use this command to configure the DAI function on the VLAN.

Use the **no** form of this command to disable this function.

ip arp inspection vlan { *vlan-id* | *word* }
no ip arp inspection vlan { *vlan-id* | *word* }

**Parameter
Description**

Parameter	Description
<i>vlan-id</i>	VLAN ID, ranging from 1 to 4094
<i>word</i>	String of the VLAN range, such as 1,3-5,7,9-11

Defaults


The DAI function on all VLANs is disabled by default.

Command Mode

Global configuration mode

Usage Guide

To make this command take effect, you need to enable the ARP Check function first,

 Not all ports of the VLAN support the ARP packet detection function. For example, the DHCP Snooping Trust port does not support any security detection, including this function.

Configuration

The following example detects the received ARP packets on the VLAN1 interfaces:

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection
Ruijie(config)# ip arp inspection vlan 1
Ruijie(config)# end
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

16.3 interface

Use this command to verify whether the interface is a DAI trust interface.

show ip arp inspection interface

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults

N/A

**Command
Mode**

Privileged EXEC mode

Usage Guide Use this command to verify whether the interface is a DAI trust interface.

Configuration The following example verifies the DAI trust state of all :

Examples Ruijie#show ip arp inspection interface

```
Interface          Trust State
-----
GigabitEthernet 0/1    Trusted
Default              Untrusted
```

Parameter Description:

Parameter	Description
Interface	Interface name.
Trust State	DAI trust state.

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

16.4 show ip arp inspection vlan

Use this command to verify whether the DAI function on the VLAN is enabled.

show ip arp inspection vlan [*vlan-id* | *word*]

**Parameter
Description**

Parameter	Description
<i>vlan-id</i>	VLAN ID, ranging from 1 to 4094
<i>word</i>	String of the VLAN range, such as 1,3-5,7,9-11

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide Use this command to verify whether the DAI function on the VLAN is enabled.

Configuration The following example verifies whether the DAI function on the VLAN is enabled:

Examples Ruijie# show ip arp inspection vlan

```
Vlan    Configuration
----    -
1                               Active
```

Parameter Description:

Parameter	Description
Vlan	VLAN number.
Configuration	DAI status (active / inactive)

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

17 IP Source Guard Commands

17.1 ip source binding

Use this command to add static user information to IP source address binding database.

Use the **no** form of this command to delete static user information from IP source address binding database.

ip source binding *mac-address* { **vlan** *vlan-id* } *ip-address* { **interface** *interface-id* | **ip-mac** | **ip-only** }

no ip source binding *mac-address* { **vlan** *vlan-id* } *ip-address* { **interface** *interface-id* | **ip-mac** | **ip-only** }

Parameter Description

Parameter	Description
<i>mac-address</i>	Adds user MAC address statically.
<i>vlan-id</i>	Adds user VLAN ID statically.
<i>ip-address</i>	Adds user IP address statically.
<i>interface-id</i>	Adds user interface ID statically.
ip-mac	The global binding type is IP+MAC
ip-only	The global binding type is IP only.

Defaults No static address is added by default.

Command Mode Global configuration mode

Usage Guide This command allows specific clients to go through IP source guard detection instead of DHCP. This command is supported on the wired L2 switching port, AP port, and sub interface. This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.

 A static IPv6 source binding is valid either on wired or in global configuration mode.

 A new binding will overwrite the old one sharing the same configuration.

Configuration

The following example adds the interface ID of static users.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface
GigabitEthernet 0/1
Ruijie(config)# end
```

The following example adds static user information based on IP-MAC binding.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
```

```
Ruijie(config)# end
```

The following example adds static user information based on IP binding.

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only
Ruijie(config)# end
```

Related Commands

Command	Description
show ip source binding	Displays the binding information of IP source address and database.

Platform Description N/A

17.2 ip verify source

Use this command to enable IP Source Guard function on the interface.

Use the **no** form of this command to restore the default setting.

ip verify source [port-security]

no ip verify source

Parameter Description


Parameter	Description
port-security	Configures IP Source Guard to do IP+MAC-based detection.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection.

This command is supported on the wired L2 switching port, AP port, and sub interface.

 IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

Configuration Examples

The following example enables IP-based IP Source Guard function.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if)# end
```

The following example enables IP+MAC-based IP Source Guard function.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# ip verify source port-security
Ruijie(config-if)# end
```

Related Commands

Command	Description
show ip verify source	Displays user filtering entry of IP Source Guard.

Platform Description

N/A

17.3 ip verify source exclude-vlan

Use this command to exclude a VLAN from the IP source guard configuration on the port.

Use the **no** form of this command to restore the function.

ip verify source exclude-vlan *vlan-id*

no ip verify source exclude-vlan *vlan-id*

Parameter Description

Parameter	Description
<i>vlan-id</i>	The ID of VLAN excluded from the IP source guard configuration.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide

- ✔ This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered.
 - ✔ Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.
 - ✔ This command is supported on the wired L2 switching port, AP port, and sub interface.
-
- i** Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.

Configuration Examples The following example configuration configures the IP source guard configuration for the port and excludes a VLAN.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
```

```
Ruijie(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
Ruijie(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform N/A**Description**

17.4 show ip source binding

Use this command to display the binding information of IP source addresses and database.

```
show ip source binding [ ip-address ] [ mac-address ] [ dhcp-snooping ] [ static ] [ vlan vlan-id ]
[ interface interface-id ]
```

Parameter Description

Parameter	Description
<i>ip-address</i>	Displays user binding information of corresponding IP.
<i>mac-address</i>	Displays user binding information of corresponding MAC.
dhcp-snooping	Displays binding information of dynamic user.
static	Displays binding information of static user.
<i>vlan-id</i>	Displays user binding information of corresponding VLAN.
<i>interface-id</i>	Displays user binding information of corresponding interface.

Defaults N/A**Command Mode** Privileged EXEC mode**Usage Guide** N/A**Configuration Examples**

The following example displays the binding information of IP source guard addresses and database.

```
Ruijie# show ip source binding static
Ruijie#show ip source binding static
Total number of bindings: 5
NO.    MACADDRESS          IPADDRESS          LEASE (SEC)    TYPE          VLAN    INTERFACE
-----
1      0001.0002.0001      1.2.3.2           Infinite       Static        1      Global
2      0001.0002.0002      1.2.3.3           Infinite       Static        1      GigabitEthernet
0/5
3      0001.0002.0003      1.2.3.4           Infinite       Static        1      Global
```

4	0001.0002.0004	1.2.3.5	Infinite	Static	1	Global
---	----------------	---------	----------	--------	---	--------

Related Commands

Command	Description
ip source binding	Sets the binding static user.

Platform N/A

Description

17.5 show ip verify source

Use this command to display user filtering entry of IP Source Guard.

show ip verify source [**interface** *interface-id*]

Parameter Description

Parameter	Description
<i>interface-id</i>	Displays user filtering entry of corresponding interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: "IP source guard is not configured on the interface FastEthernet 0/10"
Now, IP Source Guard supports the following filtering modes:

- **inactive-restrict-off**: the IP Source Guard is disabled on bound interfaces.
- **inactive--not-apply**: the IP Source Guard cannot adds bound entries into filtering entries for system errors.
- **active**: the IP Source Guard is active.

Configuration Examples The following example displays user filtering entry of IP Source Guard.

```
Ruijie # show ip verify source
Total number of bindings: 7
NO.   INTERFACE          FILTERTYPE  FILTERSTATUS  IPADDRESS
MACADDRESS  VLAN  TYPE
-----
-----
1     Global              IP+MAC     Inactive-not-apply  192.168.0.127
0001.0002.0003  1  Static
2     GigabitEthernet 0/5  IP-ONLY    Active         1.2.3.4
0001.0002.0004  1  DHCP-Snooping
3     Global              IP-ONLY    Active         1.2.3.7
0001.0002.0007  1  Static
```

```
4 Global IP+MAC Active 1.2.3.6
0001.0002.0006 1 Static
5 GigabitEthernet 0/1 UNSET Inactive-restrict-off 1.2.3.9
0001.0002.0009 1 DHCP-Snooping
6 GigabitEthernet 0/5 IP-ONLY Active Deny-All
```

**Related
Commands**

Command	Description
<code>ip verify source</code>	Sets IP Source Guard on the interface.

**Platform
Description**

N/A

18 NFPP Commands

18.1 arp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard attack-threshold { per-src-ip | per-src-mac | per-port } pps

no arp-guard attack-threshold { per-src-ip | per-src-mac | per-port }

default arp-guard attack-threshold { per-src-ip | per-src-mac | per-port }

Parameter Description	Parameter	Description
	per-src-ip	Sets the attack threshold for each source IP address.
	per-src-mac	Sets the attack threshold for each source MAC address.
	per-port	Sets the attack threshold for each port.
	<i>pps</i>	Sets the attack threshold, in the range from 1 to 19,999 in unit of pps.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command Mode NFPP configuration mode.

Usage Guide The attack threshold shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-mac 3
Ruijie(config-nfpp)# arp-guard attack-threshold per-port 50
```

Related Commands	Command	Description
	nfpp arp-guard policy	Displays the rate-limit threshold and attack threshold.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard hosts	Displays the monitored host.
	clear nfpp arp-guard hosts	Clears the isolated host.

Platform Description N/A

18.2 arp-guard enable

Use this command to enable the anti-ARP guard function globally.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard enable

no arp-guard enable

default arp-guard enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the anti-ARP guard function globally.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard enable
```

Related Commands	Command	Description
	nfpp arp-guard enable	Enables the anti-ARP attack on the interface.
	show nfpp arp-guard summary	Displays the configuration.

Platform N/A

Description

18.3 arp-guard isolate-forwarding enable

Use this command to enable packet forwarding through NFPP isolation.

Use the **no** form of this command to disable this function.

Use the **default** form of this command to restore the default setting.

arp-guard isolate-forwarding enable

no arp-guard isolate-forwarding enable

default arp-guard isolate-forwarding enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration The following example enables packet forwarding through NFPP isolation.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard isolate-forwarding enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

18.4 arp-guard isolate-period

Use this command to set the arp-guard isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard isolate-period { *seconds* | **permanent** }

no arp-guard isolate-period

default arp-guard isolate-period

Parameter Description	Parameter	Description
	<i>seconds</i>	
permanent		Permanent isolation.

Defaults The default isolate time is 0, which means no isolation.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration The following example sets the arp-guard isolate time globally to 180 seconds.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard isolate-period 180
```

Related Commands	Command	Description
	nfpp arp-guard isolate-period	Sets the isolate time on the interface.
	show nfpp arp-guard summary	Displays the configuration.

Platform N/A

Description

18.5 arp-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard monitored-host-limit *number*

no arp-guard monitored-host-limit

default arp-guard monitored-host-limit

Parameter Description	Parameter	Description
	<i>number</i>	

Defaults The default is 20000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration Examples The following example sets the maximum monitored host number to 200.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitored-host-limit 200
```

Related Commands	Command	Description
	show nfpp arp-guard summary	Displays the configuration.

Platform N/A

Description

18.6 arp-guard monitor-period

Use this command to configure the arp guard monitor time.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard monitor-period *seconds*

no arp-guard monitor-period

default arp-guard monitor-period

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600.

Command NFPP configuration mode

Mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration The following example sets the arp guard monitor time to 180 seconds.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitor-period 180
```

Related Commands	Command	Description
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard hosts	Displays the monitored host list.
	clear nfpp arp-guard hosts	Clears the isolated host.

Platform N/A

Description

18.7 arp-guard rate-limit

Use this command to set the arp guard rate limit.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard rate-limit { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

no arp-guard rate-limit { per-src-ip | per-src-mac | per-port }
default arp-guard rate-limit { per-src-ip | per-src-mac | per-port }

**Parameter
Description**

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
<i>pps</i>	Sets the rate limit, in the range of 1 to 19,999.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

**Command
Mode** NFPP configuration mode

Usage Guide N/A

Configuration The following example sets the arp guard rate limit.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard rate-limit per-src-ip 2
Ruijie(config-nfpp)# arp-guard rate-limit per-src-mac 3
Ruijie(config-nfpp)# arp-guard rate-limit per-port 50
```

**Related
Commands**

Command	Description
nfpp arp-guard policy	Sets the rate limit and the attack threshold.
show nfpp arp-guard summary	Displays the configuration.

**Platform
Description** N/A

18.8 arp-guard ratelimit-forwarding enable

Use this command to set the port based arp guard rate limit.

Use the **no** form of this command to disable this function.

Use the **default** form of this command to restore the default setting.

arp-guard ratelimit-forwarding enable

no arp-guard ratelimit-forwarding enable

default arp-guard ratelimit-forwarding enable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration The following example sets the port based arp guard rate limit.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard ratelimit-forwarding enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

18.9 arp-guard scan-threshold

Use this command to set the global scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard scan-threshold *pkt-cnt*

no arp-guard scan-threshold

default arp-guard scan-threshold

Parameter Description	Parameter	Description
	<i>pkt-cnt</i>	

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command Mode NFPP configuration mode

Usage Guide The scanning may occur on the condition that:

- More than 15 packets are received within 10 seconds;
- The source MAC address for the link layer is constant while the source IP address is uncertain;
- The source MAC and IP address for the link layer is constant while the destination IP address is uncertain.

Configuration The following example sets the global scan threshold to 20pps.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard scan-threshold 20
```

Related Commands	Command	Description
	nfpp arp-guard scan-threshold	Sets the scan threshold on the port.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard scan	Displays the ARP guard scan table.
	clear nfpp arp-guard scan	Clears the ARP guard scan table.

Platform N/A

Description

18.10 clear nfpp arp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp arp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]

Parameter Description	Parameter	Description
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
	<i>ip-address</i>	Sets the IP address.
	<i>mac-address</i>	Sets the MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears the monitored host isolation.

Examples

```
Ruijie# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	nfpp arp-guard policy	Sets the limit threshold and attack threshold.
	show nfpp arp-guard hosts	Displays the monitored host.

Platform N/A

Description

18.11 clear nfpp arp-guard scan

Use this command to clear ARP scanning table.

clear nfpp arp-guard scan

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears ARP scanning table.

Examples Ruijie# clear nfpp arp-guard scan

Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	nfpp arp-guard policy	Sets the attack threshold.
	show nfpp arp-guard scan	Displays the ARP scanning table.

Platform N/A

Description

18.12 clear nfpp define *name* hosts

Use this command to clear the monitored hosts. If the host is isolated, you need to release it.

clear nfpp define *name* hosts [vlan *vid*] [interface *interface-id*] [ip-address] [mac-address] [ipv6-address]

Parameter Description	Parameter	Description
	<i>name</i>	Defines guard name
	<i>vid</i>	VLAN ID
	<i>interface-id</i>	Interface name
	<i>ip-address</i>	IP address
	<i>ipv6-address</i>	IPv6 address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts in the self-defined range.

Configuration The following example clears the monitored hosts.

Examples

```
Ruijie# clear nfpp define tcp hosts vlan 1 interface g 0/1
```

Related Commands

Command	Description
show nfpp define hosts	Displays the isolated hosts.

Platform Description N/A

18.13 clear nfpp dhcp-guard hosts

Use this command to clear the DHCP monitored hosts, that it, release them from isolation.

clear nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description

Parameter	Description
<i>vid</i>	Sets the VLAN ID.
<i>interface-id</i>	Sets the interface name and number.
<i>mac-address</i>	Sets the MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts.

Configuration The following example clears the DHCP monitored hosts.

Examples

```
Ruijie# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
dhcp-guard attack-threshold	Sets the global attack threshold.
nfpp dhcp-guard policy	Sets the limit threshold and attack threshold.

show nfpp dhcp-guard hosts	Displays the monitored host.
-----------------------------------	------------------------------

Platform N/A

Description

18.14 clear nfpp dhcpv6-guard hosts

Use this command to clear the DHCPv6 monitored host isolation.

clear nfpp dhcpv6-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description

Parameter	Description
<i>vid</i>	Sets the VLAN ID.
<i>interface-id</i>	Sets the interface name and number.
<i>mac-address</i>	Sets the MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts

Configuration The following example clears the DHCPv6 monitored hosts.

Examples

```
Ruijie# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
dhcpv6-guard attack-threshold	Sets the global attack threshold.
nfpp dhcpv6-guard policy	Sets the limit threshold and attack threshold.
show nfpp dhcpv6-guard hosts	Displays the monitored host.

Platform N/A

Description

18.15 clear nfpp icmp-guard hosts

Use this command to clear the ICMP monitored hosts.

clear nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter Description

Parameter	Description
<i>vid</i>	Sets the VLAN ID.

<i>interface-id</i>	Sets the interface name and number.
<i>ip-address</i>	Sets the IP address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts.

Configuration The following example clears the ICMP monitored hosts.

Examples Ruijie# clear nfpp icmp-guard hosts vlan 1 interface g0/1

Related Commands

Command	Description
icmp-guard attack-threshold	Sets the global attack threshold.
nfpp icmp-guard policy	Sets the limit threshold and attack threshold.
show nfpp icmp-guard hosts	Displays the monitored host.

Platform N/A

Description

18.16 clear nfpp ip-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp ip-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter Description

Parameter	Description
<i>vid</i>	Sets the VLAN ID.
<i>interface-id</i>	Sets the interface name and number.
<i>ip-address</i>	Sets the IP address.

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide Use this command without the parameter to clear all monitored hosts.

Configuration The following example clears the monitored host isolation.

Examples Ruijie# clear nfpp ip-guard hosts vlan 1 interface g0/1

Related Commands	Command	Description
	<code>ip-guard attack-threshold</code>	Sets the global attack threshold.
	<code>nfpp ip-guard policy</code>	Sets the limit threshold and attack threshold.
	<code>show nfpp ip-guard hosts</code>	Displays the monitored host.

Platform N/A

Description

18.17 clear nfpp log

Use this command to clear the NFPP log buffer area.

clear nfpp log

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Privileged EXEC mode
Mode

Usage Guide N/A

Configuration The following example clears the NFPP log buffer area.

Examples

```
Ruijie# clear nfpp log
```

Related Commands	Command	Description
	<code>show nfpp log</code>	Displays the NFPP log configuration or the log buffer area.

Platform N/A

Description

18.18 clear nfpp nd-guard hosts

Use this command to remove the speed limit on the monitored host.

clear nfpp nd-guard hosts [vlan *vid*] [interface *interface-id*]

Parameter Description	Parameter	Description

<i>vid</i>	Sets the VLAN ID.
<i>interface-id</i>	Sets the interface name and number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command without any parameter is used to remove speed limit on all monitored hosts.

Configuration Examples The following example removes speed limit on interface g0/1 in VLAN 1.

```
Ruijie# clear nfpp nd-guard hosts vlan 1 interface g0/1
```

Prompt Messages N/A

Platform Description

Platform N/A

Description

18.19 cpu-protect sub-interface { manage | protocol | route } percent

Use this command to configure the percent value of each type of packets occupied in the buffer area.

Use the **no** or **default** form of this command to restore the default setting.

cpu-protect sub-interface { manage | protocol | route } percent *percent_value*

no cpu-protect sub-interface { manage | protocol | route } percent

default cpu-protect sub-interface { manage | protocol | route } percent

Parameter Description	Parameter	Description
	<i>percent_value</i>	The percent value, in the range from 1 to 100.

Defaults The default percent values of each type of packets occupied in the buffer area are:

Manage packets: 30;

Route packets: 25;

Protocol packets: 45.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the percent value of management packets in the buffer area to 60.

```
Ruijie(config)# cpu-protect sub-interface manage percent 60
```

Related Commands	Command	Description
		cpu-protect sub-interface { manage protocol route } pps

Platform N/A
Description

18.20 cpu-protect sub-interface { manage | protocol | route } pps

Use this command to configure the traffic bandwidth of each type of packets.

Use the **no** or **default** form of this command to restore the default setting.

cpu-protect sub-interface { manage | protocol | route } pps pps_value

no cpu-protect sub-interface { manage | protocol | route } pps

default cpu-protect sub-interface { manage | protocol | route } pps

Parameter Description	Parameter	Description
		<i>pps_value</i>

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the traffic bandwidth of management packets to 2,000 pps.

```
Ruijie(config)# cpu-protect sub-interface manage pps 2000
```

Related Commands	Command	Description
		cpu-protect sub-interface { manage protocol route } percent

Platform N/A
Description

18.21 define

Use this command to define the anti-attack type.

Use the **no** or **default** form of this command to restore the default setting.

define *name*

no define *name*

default define *name*

Parameter Description	Parameter	Description
	<i>name</i>	Name of the user-defined anti-attack type

Defaults N/A

Command Mode NFPP configuration mode

Usage Guide Use this command to define the anti-attack type.

Configuration The following example creates the user-defined anti-attack type.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
Ruijie(config-nfpp-define)#
```

Related Commands	Command	Description
	show nfpp define summary	Displays the defined anti-attack configuration.

Platform Description N/A

18.22 define *name* enable

Use this command to enable the user-defined anti-attack globally.

Use the **no** or **default** form of this command to restore the default setting.

define *name* **enable**

no define *name* **enable**

default define *name* **enable**

Parameter Description	Parameter	Description
	<i>name</i>	Defines guard name.

Defaults This function is disabled by default.

Command Mode NFPP configuration mode

Usage Guide This command takes effect only after the match, rate-limit and attack-threshold have been configured.

Configuration The following example enabled the user-defined anti-attack globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#define tcp enable
```

Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration

Platform N/A

Description

18.23 dhcp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

```
dhcp-guard attack-threshold { per-src-mac | per-port } pps
no dhcp-guard attack-threshold { per-src-mac | per-port }
default dhcp-guard attack-threshold { per-src-mac | per-port }
```

Parameter Description	Parameter	Description
	per-src-mac	Sets the attack threshold for each source MAC address.
	per-port	Sets the attack threshold for each port.
	<i>pps</i>	Sets the attack threshold, in pps. The valid range is 1 to 19,999.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration The following example sets the global attack threshold.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

Related	Command	Description
---------	---------	-------------

Commands	
nfpp dhcp-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp dhcp-guard summary	Displays the configuration.
show nfpp dhcp-guard hosts	Displays the monitored host list.
clear nfpp dhcp-guard hosts	Clears the monitored host.

Platform N/A

Description

18.24 dhcp-guard enable

Use this command to enable the DHCP anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard enable

no dhcp-guard enable

default dhcp-guard enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the DHCP anti-attack function.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

18.25 dhcp-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

```
dhcp-guard isolate-period { seconds | permanent }
no dhcp-guard isolate-period
default dhcp-guard isolate-period
```

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate time. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation.

Defaults The default isolate time is 0, which means no isolation.

Command Mode NFPP configuration mode

Usage Guide The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Configuration Examples The following example sets the isolate time globally to 180 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard isolate-period 180
```

Related Commands	Command	Description
	nfpp dhcp-guard isolate-period	Sets the isolate time on the interface.
	show nfpp dhcp-guard summary	Displays the configuration.

Platform Description N/A

18.26 dhcp-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

```
dhcp-guard monitored-host-limit number
no dhcp-guard monitored-host-limit
default dhcp-guard monitored-host-limit
```

Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration The following example sets the maximum monitored host number to 200.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp dhcp-guard summary	Displays the configuration.

Platform N/A

Description

18.27 dhcp-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard monitor-period *seconds*

no dhcp-guard monitor-period

default dhcp-guard monitor-period

Parameter Description

Parameter	Description
<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600 seconds.

Command Mode NFPP configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software

and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration The following example sets the monitor time to 180 seconds.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitor-period 180
```

**Related
Commands**

Command	Description
show nfpp dhcp-guard summary	Displays the configuration.
show nfpp dhcp-guard hosts	Displays the monitored host list.
clear nfpp dhcp-guard hosts	Clears the isolated host.

Platform N/A

Description

18.28 dhcp-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard rate-limit { per-src-mac | per-port } pps

no dhcp-guard rate-limit { per-src-mac | per-port }

default dhcp-guard rate-limit { per-src-mac | per-port }

**Parameter
Description**

Parameter	Description
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
<i>pps</i>	Sets the rate limit, in the range of 1 to 19,999.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command NFPP configuration mode

Mode

Usage Guide N/A

Configuration The following example sets the rate-limit threshold globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
```

```
Ruijie(config-nfpp)# dhcp-guard rate-limit per-port 100
```

**Related
Commands**

Command	Description
nfpp dhcp-guard policy	Sets the rate limit and the attack threshold.
show nfpp dhcp-guard summary	Displays the configuration.

Platform N/A
Description

18.29 dhcpv6-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard attack-threshold { per-src-mac | per-port } pps

no dhcpv6-guard attack-threshold { per-src-mac | per-port }

default dhcpv6-guard attack-threshold { per-src-mac | per-port }

**Parameter
Description**

Parameter	Description
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
<i>pps</i>	Sets the attack threshold, in the range is from 1 to 19,999 pps.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command Mode NFPP configuration mode

Usage Guide N/A.

Configuration Examples The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

**Related
Commands**

Command	Description
nfpp dhcpv6-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.

show nfpp dhcpv6-guard hosts	Displays the monitored host list.
clear nfpp dhcpv6-guard hosts	Clears the monitored host.

Platform N/A

Description

18.30 dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard enable

no dhcpv6-guard enable

default dhcpv6-guard enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command NFPP configuration mode

Mode

Usage Guide N/A

Configuration The following example enables the DHCPv6 anti-attack function globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

18.31 dhcpv6-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard monitored-host-limit *number*

no dhcpv6-guard monitored-host-limit

default dhcpv6-guard monitored-host-limit

Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration The following example sets the maximum monitored host number to 200.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard monitored-host-limit 200
```

Related Commands	Command	Description
	show nfpp dhcpv6-guard summary	Displays the configuration.

Platform N/A
Description

18.32 dhcpv6-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard monitor-period *seconds*

no dhcpv6-guard monitor-period

default dhcpv6-guard monitor-period

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600 seconds.

Command NFPP configuration mode
Mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
 If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration The following example sets the monitor time to 180 seconds.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard monitor-period 180
```

Related Commands	Command	Description
	<code>show nfpp dhcpv6-guard summary</code>	Displays the configuration.
<code>show nfpp dhcpv6-guard hosts</code>	Displays the monitored host list.	
<code>clear nfpp dhcpv6-guard hosts</code>	Clears the isolated host.	

Platform N/A
Description

18.33 dhcpv6-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard rate-limit { per-src-mac | per-port } pps

no dhcpv6-guard rate-limit { per-src-mac | per-port }

default dhcpv6-guard rate-limit { per-src-mac | per-port }

Parameter Description	Parameter	Description
	<code>per-src-mac</code>	Sets the rate limit for each source MAC address.
<code>per-port</code>	Sets the rate limit for each port.	
<code>pps</code>	Sets the rate limit, in the range from 1 to 19,999.	

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command NFPP configuration mode
Mode

Usage Guide N/A

Configuration The following example sets the rate-limit threshold globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-port 100
```

**Related
Commands**

Command	Description
nfpp dhcpv6-guard policy	Sets the rate limit and the attack threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.

Platform N/A

Description

18.34 global-policy

Use this command to set the rate-limit threshold and attack threshold based on the host or port.

Use the **no** or **default** form of this command to restore the default setting.

global-policy { **per-src-mac** | **per-src-ip** | **per-port** } *rate-limit-pps* *attack-threshold-pps*

no global-policy { **per-src-mac** | **per-src-ip** | **per-port** }

default global-policy { **per-src-mac** | **per-src-ip** | **per-port** }

**Parameter
Description**

Parameter	Description
per-src-ip	Performs the rate statistics based on the source IP / VID and port.
per-src-mac	Performs the rate statistics based on the source MAC / VID and port.
per-port	Performs the rate statistics based on each physical port of receiving the packets.
<i>rate-limit-pps</i>	Sets the rate-limit threshold.
<i>attack-threshold-pps</i>	Sets the attack threshold.

Defaults By default, no rate-limit threshold and attack threshold is configured. To enable self-defined anti-attack, these two parameters must be set.

Command NFPP define configuration mode

Mode

Usage Guide To create a user-defined anti-attack type, the classification rule for the rate statistics must be specified, that is, recognize the host based on the source IP address/ source MAC address for the user-defined packets rate statistics based on the user / port and specify the rate-limit threshold and attack threshold for each classification. The rate-limit threshold shall be equal to or greater than the attack threshold. If the rate is greater than the rate-limit threshold, the packets that meet this classification rule will be discarded. If the rate exceeds the attack threshold, the user will be regarded

as an attacker. The log will be printed and the trap will be sent.

Configuration The following example sets the rate-limit threshold and attack threshold based on the host or port.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)# global-policy per-src-ip 10 20
Ruijie(config-nfpp-define)# global-policy per-port 100 200
```

**Related
Commands**

Command	Description
nfpp define <i>name</i> policy	Sets the rate-limit threshold and attack threshold.
show nfpp define summary	Displays the user-defined anti-attack configuration

Platform N/A

Description

18.35 icmp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard attack-threshold { **per-src-ip** | **per-port** } *pps*

no icmp-guard attack-threshold { **per-src-ip** | **per-port** }

default icmp-guard attack-threshold { **per-src-ip** | **per-port** }

**Parameter
Description**

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-port	Sets the attack threshold for each port.
<i>pps</i>	Sets the attack threshold, in the range from 1 to 19,999 in the unit of pps.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

**Command
Mode** NFPP configuration mode

Usage Guide N/A

Configuration The following example sets the global attack threshold.

Examples

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
Ruijie(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

**Related
Commands**

Command	Description
nfpp icmp-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host list.
clear nfpp icmp-guard hosts	Clears the monitored host.

Platform N/A**Description**

18.36 icmp-guard enable

Use this command to enable the ICMP anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard enable

no icmp-guard enable

default icmp-guard enable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.**Command** NFPP configuration mode**Mode****Usage Guide** N/A**Configuration** The following example enables the ICMP anti-attack function globally.**Examples**

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard enable
```

**Related
Commands**

Command	Description
nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
show nfpp icmp-guard summary	Displays the configuration.

Platform N/A

Description

18.37 icmp-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard isolate-period { *seconds* | **permanent** }

no icmp-guard isolate-period

default icmp-guard isolate-period

**Parameter
Description**

Parameter	Description
<i>seconds</i>	Sets the isolate time. The value is in the range is 0 or from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation.

Defaults The default isolate time is 0, which means no isolation.

Command NFPP configuration mode

Mode

Usage Guide The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Configuration The following example sets the isolate time globally to 180 seconds.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard isolate-period 180
```

**Related
Commands**

Command	Description
nfpp icmp-guard isolate-period	Sets the isolate time on the interface.
show nfpp icmp-guard summary	Displays the configuration.

Platform N/A

Description

18.38 icmp-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard monitored-host-limit *number*

no icmp-guard monitored-host-limit
default icmp-guard monitored-host-limit

Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.

Configuration The following example sets the maximum monitored host number to 200.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitored-host-limit 200
```

Related Commands	Command	Description
	show nfpp icmp-guard summary	Displays the configuration.

Platform N/A
Description

18.39 icmp-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard monitor-period *seconds*
no icmp-guard monitor-period
default icmp-guard monitor-period

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 seconds.

Defaults The default is 600.

Command Mode NFPP configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration The following example sets the monitor time to 180 seconds.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host list.
clear nfpp icmp-guard hosts	Clears the isolated host.

Platform N/A

Description

18.40 icmp-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard rate-limit { per-src-ip | per-port } pps

no icmp-guard rate-limit { per-src-ip | per-port }

default icmp-guard rate-limit { per-src-ip | per-port }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-port	Sets the rate limit for each port.
<i>pps</i>	Sets the rate limit, in the range from 1 to 19,999.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration The following example sets the rate-limit threshold globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard rate-limit per-src-ip 500
Ruijie(config-nfpp)# icmp-guard rate-limit per-port 800
```

**Related
Commands**

Command	Description
nfpp icmp-guard policy	Sets the rate limit and the attack threshold.
show nfpp icmp-guard summary	Displays the configuration.

Platform N/A

Description

18.41 icmp-guard trusted-host

Use this command to set the trusted hosts free form monitoring.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard trusted-host *ip mask*

no icmp-guard trusted-host { **all** | *ip mask* }

default icmp-guard trusted-host

**Parameter
Description**

Parameter	Description
<i>ip</i>	Sets the IP address.
<i>mask</i>	Sets the IP mask.
all	Deletes the configuration of all trusted hosts.

Defaults No trusted host is configured by default.

Command NFPP configuration mode

Mode

Usage Guide The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to send to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.

Configuration The following example sets the trusted hosts free form monitoring.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

Related Commands	Command	Description
		<code>show nfpp icmp-guard trusted-host</code>

Platform N/A
Description

18.42 ip-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard attack-threshold { **per-src-ip** | **per-port** } *pps*

no ip-guard attack-threshold { **per-src-ip** | **per-port** }

default ip-guard attack-threshold { **per-src-ip** | **per-port** }

Parameter Description	Parameter	Description
		per-src-ip
	per-port	Sets the attack threshold for each port.
	<i>pps</i>	Sets the attack threshold, in pps. The valid range is 1 to 19,999.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command Mode NFPP configuration mode

Usage Guide The attack threshold shall be equal to or larger than the rate-limit threshold.

Configuration Examples The following example sets the global attack threshold.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard attack-threshold per-src-ip 2
Ruijie(config-nfpp)# ip-guard attack-threshold per-port 50
```

Related Commands	Command	Description
		nfpp ip-guard policy
	show nfpp ip-guard summary	Displays the configuration.
	show nfpp ip-guard hosts	Displays the monitored host list.
	clear nfpp ip-guard hosts	Clears the monitored host.

Platform N/A

Description

18.43 ip-guard enable

Use this command to enable IP guard.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard enable

no ip-guard enable

default ip-guard enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is enabled by default.

Command NFPP configuration mode.

Mode

Usage Guide This configuration aims at attacks whose destination IP address is not the local one. For those with the local address as the destination, CPP (CPU Protect Policy) will limit their rates.

Configuration The following example enables the IP guard globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard enable
```

Related Commands	Command	Description
	nfpp ip-guard enable	Enables the IP guard on the interface.

Platform N/A

Description

18.44 ip-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard isolate-period { seconds | permanent }

no ip-guard isolate-period

default ip-guard isolate-period

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
<i>seconds</i>	Sets the isolate time. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation

Defaults The default isolate time is 0 second, which means no isolation.

Command NFPP configuration mode

Mode

Usage Guide N/A.

Configuration The following example sets the isolate time globally to 180 seconds.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard isolate-period 180
```

Related Commands	Command	Description
	nfpp ip-guard isolate-period	Sets the isolate time on the interface.
show nfpp ip-guard summary	Displays the configuration.	

Platform N/A

Description

18.45 ip-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard monitored-host-limit *number*

no ip-guard monitored-host-limit

default ip-guard monitored-host-limit

Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000 seconds.

Command NFPP configuration mode

Mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you

configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.

Configuration The following example sets the maximum monitored host number to 200.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard monitored-host-limit 200
```

**Related
Commands**

Command	Description
show nfpp ip-guard summary	Displays the configuration.

Platform N/A

Description

18.46 ip-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard monitor-period *seconds*

no ip-guard monitor-period

default ip-guard monitor-period

**Parameter
Description**

Parameter	Description
<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600 seconds.

Command NFPP configuration mode

Mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software

Configuration The following example sets the monitor time to 180 seconds.

Examples

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# ip-guard monitor-period 180
```

**Related
Commands**

Command	Description
show nfpp ip-guard summary	Displays the configuration.
show nfpp ip-guard hosts	Displays the monitored host list.
clear nfpp ip-guard hosts	Clears the isolated host.

Platform N/A

Description

18.47 ip-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

```
ip-guard rate-limit { per-src-ip | per-port } pps
```

```
no ip-guard rate-limit { per-src-ip | per-port }
```

```
default ip-guard rate-limit {per-src-ip | per-port }
```

**Parameter
Description**

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-port	Sets the rate limit for each port.
<i>pps</i>	Sets the rate limit, in the range of 1 to 19,999.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command NFPP configuration mode

Mode
Usage Guide N/A

Configuration The following example sets the rate-limit threshold globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard rate-limit per-src-ip 2
Ruijie(config-nfpp)# ip-guard rate-limit per-port 50
```

**Related
Commands**

Command	Description
nfpp ip-guard policy	Sets the rate limit and the attack threshold.
show nfpp ip-guard summary	Displays the configuration.

Platform N/A

Description

18.48 ip-guard scan-threshold

Use this command to set the global scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard scan-threshold *pkt-cnt*

no ip-guard scan-threshold

default ip-guard scan-threshold

**Parameter
Description**

Parameter	Description
<i>pkt-cnt</i>	Sets the scan threshold, in the range from 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

**Command
Mode**

NFPP configuration mode.

Usage Guide

N/A

Configuration

The following example sets the global scan threshold to 20 pps.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard scan-threshold 20
```

**Related
Commands**

Command	Description
nfpp ip-guard scan-threshold	Sets the scan threshold on the port.
show nfpp ip-guard summary	Displays the configuration.

Platform

N/A

Description

18.49 ip-guard trusted-host

Use this command to set the trusted hosts free form monitoring.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard trusted-host *ip mask*

no ip-guard trusted-host { **all** | *ip mask* }

default ip-guard trusted-host

Parameter Description	Parameter	Description
	<i>ip</i>	Sets the IP address.
	<i>mask</i>	Sets the IP mask.
	all	Deletes the configuration of all trusted hosts.

Defaults N/A

Command Mode NFPP configuration mode

Usage Guide The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.

Configuration The following example sets the trusted hosts free form monitoring.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard trusted-host 1.1.1.0 255.255.255.0
```

Related Commands	Command	Description
	show nfpp ip-guard trusted-host	Displays the configuration.

Platform Description N/A

18.50 log-buffer enable

Use this command to display logs on the screen.

Use the **no** or the **default** form of this command to restore the default setting.

log-buffer enable

no log-buffer enable

default log-buffer enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Logs are stored in the cache by default.

Command Mode NFPP configuration mode

Usage Guide N/A

Configuration The following example displays logs on the screen.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer enable
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

18.51 log-buffer entries

Use this command to set the NFPP log buffer area size.

Use the **no** or **default** form of this command to restore the default setting.

log-buffer entries *number*

no log-buffer entries

default log-buffer entries

**Parameter
Description**

Parameter	Description
<i>number</i>	The buffer area size, in the range from 0 to 1,024.

Defaults The default is 256.

**Command
Mode** NFPP configuration mode

Usage Guide N/A

Configuration The following example sets the NFPP log buffer area size.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer entries 50
```

**Related
Commands**

Command	Description
log-buffer logs <i>number_of_message</i> interval <i>length_in_seconds</i>	Displays the rate of the syslog generated from the NFPP buffer area.
show nfpp log	Displays the NFPP log configuration or the log buffer area.

Platform N/A

Description

18.52 log-buffer logs

Use this command to set the rate of syslog generated from the NFPP log buffer area.

Use the **no** or **default** form of this command to restore the default setting.

log-buffer logs *number_of_message* **interval** *length_in_seconds*

no log-buffer logs

default log-buffer logs

Parameter Description	Parameter	Description
	<i>number_of_message</i>	The valid range is from 0 to 1024. 0 indicates that all logs are recorded in the specific buffer area and no syslogs are generated.
	<i>length_in_seconds</i>	The valid range is from 0 to 86400(one day). 0 indicates not to write the log to the buffer area but generate the syslog immediately. With both the <i>number_of_message</i> and <i>length_in_seconds</i> values are 0, it indicates not to write the log to the buffer area but generate the syslog immediately. The parameter <i>number_of_message /length_in_second</i> indicates the rate of syslog generated from the NFPP log buffer area.

Defaults By default, *number_of_message* is 0 and *length_in_seconds* is 0.

Command NFPP configuration mode

Mode

Usage Guide N/A

Configuration The following example sets the rate of syslog generated from the NFPP log buffer area.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer logs 2 interval 12
```

Related Commands

Command	Description
log-buffer entries <i>number</i>	Sets the NFPP log buffer area size.
show nfpp log summary	Displays the NFPP log configuration or the log buffer area.

Platform N/A

Description

18.53 logging

Use this command to set the VLAN or the interface log for NFPP.

Use the **no** or **default** form of this command to restore the default setting.

logging vlan *vlan-range*

logging interface *interface-id*

no logging vlan *vlan-range*

no logging interface *interface-id*

default logging

Parameter Description	Parameter	Description
	<i>vlan-range</i>	Sets the specified VLAN range, in the format such as "1-3, 5".
	<i>interface-id</i>	Sets the interface ID.

Defaults All logs are recorded by default.

Command NFPP configuration mode

Mode

Usage Guide Use this command to filter the logs and records the logs within the specified VLAN range or the specified port

Configuration The following example records the logs in VLAN 1, VLAN 2,VLAN 3 and VLAN 5 only.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# logging vlan 1-3,5
```

The following example records the logs on the interface GigabitEthernet 0/1 only.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# logging interface G 0/1
```

Related Commands	Command	Description
	show nfpp log summary	Displays the NFPP log configuration or the log buffer area.

Platform N/A

Description

18.54 match

Use this command to specify the message matching filed for the user-defined anti-attack.

match [*etype type*] [**src-mac** *smac* [**src-mac-mask** *smac_mask*]] [**dst-mac** *dmac*

[**dst-mac-mask** *dst_mask*] [**protocol** *protocol*] [**src-ip** *sip* [**src-ip-mask** *sip-mask*]] [**src-ipv6** *sipv6* [**src-ipv6-masklen** *sipv6-masklen*]] [**dst-ip** *dip* [**dst-ip-mask** *dip-mask*]] [**dst-ipv6** *dipv6* [**dst-ipv6-masklen** *dipv6-masklen*]] [**src-port** *sport*] [**dst-port** *dport*]

Parameter Description	Parameter	Description
	<i>type</i>	Ethernet link layer packet type
	<i>smac</i>	Source MAC address
	<i>smac_mask</i>	Source MAC address mask
	<i>dmac</i>	Destination MAC address
	<i>dmac_mask</i>	Destination MAC address mask
	<i>protocol</i>	IPv4/v6 message protocol
	<i>sip</i>	Source IPv4 address
	<i>sip_mask</i>	Source IPv4 address mask
	<i>sipv6</i>	Source IPv6 address
	<i>sipv6_masklen</i>	Source IPv6 address mask
	<i>dip</i>	Destination IPv4 address
	<i>dip_mask</i>	Destination IPv4 address mask
	<i>dipv6</i>	Destination IPv6 address
	<i>dipv6_masklen</i>	Length of the destination IPv6 address mask.
	<i>sport</i>	Source port
	<i>dport</i>	Destination port

Defaults N/A

Command Mode NFPP configuration mode

Usage Guide Use this command to create a new user-defined anti-attack type and specify the message fields to be matched.

Configuration Examples The following example specifies the message matching filed for the user-defined anti-attack.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)#match etype 0x0800 protocol 0x06
```

Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description N/A

18.55 monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

monitored-host-limit *number*

no monitored-host-limit

default monitored-host-limit

Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults The default is 20,000.

Command Mode NFPP define configuration mode

Usage Guide If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that % % NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 20,000 monitored hosts. to remind the administrator

Configuration The following example sets the maximum monitored host number.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)#monitored-host-limit 500
```

Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description N/A

18.56 monitor period

Use this command to set the monitoring time.

Use the **no** or **default** form of this command to restore the default setting.

monitor-period *seconds*
no monitor-period
default monitor-period

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults The default is 600 seconds.

Command Mode NFPP define configuration mode

Usage Guide When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
 If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples The following example sets the monitoring time to 1,000 seconds.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
Ruijie(config-nfpp-define)#monitor-period 1000
```

Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform Description N/A

18.57 nd-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard attack-threshold per-port { ns-na | rs | ra-redirect } pps
no nd-guard attack-threshold per-port { ns-na | rs | ra-redirect }
default nd-guard attack-threshold per-port { ns-na | rs | ra-redirect }

Parameter	Parameter	Description
-----------	-----------	-------------

Description	
ns-na	Sets the neighbor request and neighbor advertisement.
rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
<i>pps</i>	Sets the attack threshold, in the range from 1 to 19999 in the unit of seconds.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command NFPP configuration mode.

Mode

Usage Guide The attack threshold shall be equal to or larger than the rate-limit threshold.

Configuration The following example sets the global attack threshold.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Ruijie(config-nfpp)# nd-guard attack-threshold per-port rs 10
Ruijie(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
```

Related Commands	Command	Description
	nfpp ip-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Displays the configuration.	

Platform N/A

Description

18.58 nd-guard enable

Use this command to enable the ND anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard enable

no nd-guard enable

default nd-guard enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command NFPP configuration mode
Mode

Usage Guide N/A

Configuration The following example enables the ND anti-attack function.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard enable
```

**Related
Commands**

Command	Description
nfpp nd-guard enable	Enables the ND anti-attack function on the interface.
show nfpp nd-guard summary	Displays the configuration.

Platform N/A

Description

18.59 nd-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard rate-limit per-port { ns-na | rs | ra-redirect } pps

no nd-guard rate-limit per-port { ns-na | rs | ra-redirect }

default nd-guard rate-limit per-port { ns-na | rs | ra-redirect }

**Parameter
Description**

Parameter	Description
ns-na	Sets the neighbor request and neighbor advertisement.
rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
<i>pps</i>	Sets the attack threshold, in the range is from 1 to 19,999 in the unit of pps.

Defaults The default value varies with products. For details, see the *Configuration Guide*.

Command NFPP configuration mode
Mode

Usage Guide N/A

Configuration The following example sets the rate-limit threshold globally.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard rate-limit per-port ns-na 10
```

```
Ruijie(config-nfpp)# nd-guard rate-limit per-port rs 5
Ruijie(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
```

**Related
Commands**

Command	Description
nfpp nd-guard policy	Sets the rate limit and the attack threshold.
show nfpp nd-guard summary	Displays the configuration.

Platform N/A**Description**

18.60 nd-guard ratelimit-forwarding enable

Use this command to enable the ND-guard ratelimit-forwarding on the interface.

nd-guard ratelimit-forwarding enable

Use this command to disable the ND-guard ratelimit-forwarding on the interface.

no nd-guard ratelimit-forwarding enable

Use this command to restore the default setting.

default nd-guard ratelimit-forwarding enable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults The function is enabled by default.**Command
Mode** NFPP configuration mode**Usage Guide** N/A**Configuration** The following example enables the ND-guard ratelimit-forwarding on the interface.

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard ratelimit-forwarding enable
```

Platform N/A**Description**

18.61 nfpp

Use this command to enter NFPP configuration mode.

nfpp

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enter NFPP configuration mode and make further configuration.	
Configuration Examples	The following example enters NFPP configuration mode.	
	<pre>Ruijie(config)# nfpp</pre>	
Platform Description	N/A	

18.62 nfpp arp-guard enable

Use this command to enable the anti-ARP attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard enable

no nfpp arp-guard enable

default nfpp arp-guard enable

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The anti-ARP attack function is not enabled on the interface.	
Command Mode	Interface configuration mode	
Usage Guide	The interface anti-ARP attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the anti-ARP attack function on the interface.	
	<pre>Ruijie(config)# interface G0/1 Ruijie(config-if)# nfpp arp-guard enable</pre>	
Related	Command	Description

Commands	
arp-guard enable	Enables the anti-ARP attack function.
show nfpp arp-guard summary	Displays the configuration.

Platform N/A

Description

18.63 nfpp arp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard isolate-period { *seconds* | **permanent** }

no nfpp arp-guard isolate-period

default nfpp arp-guard isolate-period

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate period. The value is 0, or in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation

Defaults By default, the isolate period is not configured.

Command Mode Interface configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example sets the isolate period in the interface configuration mode.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp arp-guard isolate-period 180
```

Related Commands	Command	Description
	arp-guard isolate-period	Sets the global isolate period.
	show nfpp arp-guard summary	Displays the configuration.

Platform N/A

Description

18.64 nfpp arp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

```

nfpp arp-guard policy { per-src-ip | per-src-mac | per-port } rate-limit-pps attack-threshold-pps
no nfpp arp-guard policy { per-src-ip | per-src-mac | per-port }
default nfpp arp-guard policy { per-src-ip | per-src-mac | per-port }

```

Parameter Description	Parameter	Description
	per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
	per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from 1 to 19999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples The following example sets the rate-limit threshold and the attack threshold.

```

Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard policy per-src-ip 2 10
Ruijie(config-if)# nfpp arp-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp arp-guard policy per-port 50 100

```

Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	arp-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard hosts	Displays the monitored host.
	clear nfpp arp-guard hosts	Clears the isolated host.

Platform Description N/A

18.65 nfpp arp-guard scan-threshold

Use this command to set the scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard scan-threshold *pkt-cnt*
no nfpp arp-guard scan-threshold
default nfpp arp-guard scan-threshold

Parameter Description	Parameter	Description
	<i>pkt-cnt</i>	Sets the scan threshold, in the range from 1 to 19,999.

Defaults By default, the sport-based scan threshold is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the scan threshold to 20 pps.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard scan-threshold 20
```

Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard scan	Displays the ARP scan table.
	clear nfpp arp-guard scan	Clears the ARP scan table.

Platform Description N/A

18.66 nfpp define *name* enable

Use this command to enable the user-defined anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp define *name* **enable**
no nfpp define *name* **enable**
default nfpp define *name* **enable**

Parameter Description	Parameter	Description
	<i>name</i>	Name of the user-defined anti-attack type

Defaults N/A

Command Interface configuration mode.
Mode

Usage Guide This command takes effect only after the name of the user-defined anti-attack and the match, rate-count, rate-limit and the attack-threshold have been configured.

Configuration The following example enables the user-defined anti-attack function on the interface.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp define tcp enable
```

**Related
Commands**

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform N/A
Description

18.67 nfpp define *name* isolate-period

Use this command to set the local isolation time in the interface configuration mode.

```
nfpp define name isolate-period { seconds | permanent }
no nfpp define name isolate-period
default nfpp define name isolate-period
```

**Parameter
Description**

Parameter	Description
<i>seconds</i>	Sets the isolation time, in second. The valid range is 0, or [30, 86,400]. 0 indicates no isolation.
<i>name</i>	Name of the user-defined anti-attack type.
permanent	Permanent isolation.

Defaults By default, the local isolation time is not configured. The global isolation time is used.

Command Interface configuration mode
Mode

Usage Guide N/A

Configuration The following example shows how to set the local isolation time in the interface configuration mode.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp define tcp isolate-period 180
```

**Related
Commands**

Command	Description
---------	-------------

isolate-period	Sets the global isolation time.
show nfpp define summary	Displays the configurations.

Platform N/A

Description

18.68 nfpp define name policy

Use this command to set the local rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp define name policy { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps* *attack-threshold-pps*

no nfpp define name policy {**per-src-ip** | **per-src-mac** | **per-port**}

default nfpp define name policy { **per-src-ip** | **per-src-mac** | **per-port** }

Parameter Description	Parameter	Description
	per-src-ip	Sets the attack threshold for each source IP address.
	per-src-mac	Sets the attack threshold for each source MAC address.
	per-port	Sets the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range of from 1 to 19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Interface configuration mode

Mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration The following example sets the local rate-limit threshold and the attack threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp define tcp policy per-src-ip 2 10
Ruijie(config-if)# nfpp define tcp policy per-port 50 100
```

Related Commands	Command	Description
	define-policy	Sets the global rate-limit threshold and attack threshold.
	show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform N/A

Description

18.69 nfpp dhcp-guard enable

Use this command to enable the DHCP anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp dhcp-guard enable

no nfpp dhcp-guard enable

default nfpp dhcp-guard enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The DHCP anti-attack function is not enabled on the interface.

Command Mode Interface configuration mode

Usage Guide The interface DHCP anti-attack configuration is prior to the global configuration

Configuration Examples The following example enables the DHCP anti-attack function on the interface.

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcp-guard enable
```

Related Commands	Command	Description
	dhcp-guard enable	Enables the anti-ARP attack function.
	show nfpp dhcp-guard summary	Displays the configuration.

Platform N/A

Description

18.70 nfpp dhcp-guard policy

Use this command to set the rate-limit threshold and the attack threshold on the port.

Use the **no** or **default** form of this command to restore the default setting.

nfpp dhcp-guard policy { per-src-mac | per-port } rate-limit-pps attack-threshold-pps

no nfpp dhcp-guard policy { per-src-mac | per-port }

default nfpp dhcp-guard policy { per-src-mac | per-port }

Parameter Description	Parameter	Description
	per-src-mac	Sets the rate-limit threshold and the attack threshold for the designated source MAC address.

per-port	Sets the rate-limit threshold and the attack threshold for the designated port.
<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from 1 to 19,999.

Defaults The rate-limit threshold and the attack threshold are not configured by default. So the device adopts the rate-limit threshold and the attack threshold that are set in the global configuration mode.

Command Interface configuration mode

Mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration The following example sets the rate-limit threshold and the attack threshold on interface G0/1.

Examples

```
Ruijie(config)#interface G 0/1
Ruijie(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

18.71 nfpp dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp dhcpv6-guard enable

no nfpp dhcpv6-guard enable

default nfpp dhcpv6-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The DHCPv6 anti-attack function is not enabled on the interface.

Command Interface configuration mode

Mode

Usage Guide The interface DHCPv6 anti- attack configuration is prior to the global configuration.

Configuration The following example enables the DHCPv6 anti-attack function on interface G0/1.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcpv6-guard enable
```

Related Commands	Command	Description
	dhcpv6-guard enable	Enables the anti-ARP attack function.
	show nfpp dhcpv6-guard summary	Displays the configuration.

Platform N/A

Description

18.72 nfpp dhcpv6-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp dhcpv6-guard policy { per-src-mac | per-port } rate-limit-pps attack-threshold-pps

no nfpp dhcpv6-guard policy { per-src-mac | per-port }

default nfpp dhcpv6-guard policy { per-src-mac | per-port }

Parameter Description	Parameter	Description
	per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range of from1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from1 to19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode Interface configuration mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration The following example sets the rate-limit threshold and the attack threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related Commands	Command	Description
	dhcpv6-guard attack-threshold	Sets the global attack threshold.

dhcpv6-guard rate-limit	Sets the global rate-limit threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored host.
clear nfpp dhcpv6-guard hosts	Clears the isolated host.

Platform N/A

Description

18.73 nfpp icmp-guard enable

Use this command to enable the ICMP anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp icmp-guard enable

no nfpp icmp-guard enable

default nfpp icmp-guard enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The ICMP anti-attack function is not enabled on the interface.

Command Interface configuration mode

Mode

Usage Guide The interface ICMP anti- attack configuration is prior to the global configuration.

Configuration The following example enables the ICMP anti-attack function on the interface.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp icmp-guard enable
```

Related Commands	Command	Description
	icmp-guard enable	Enables the anti-ARP attack function.
	show nfpp icmp-guard summary	Displays the configuration.

Platform N/A

Description

18.74 nfpp icmp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

```

nfpp icmp-guard isolate-period { seconds | permanent }
no nfpp icmp-guard isolate-period
default nfpp icmp-guard isolate-period

```

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate period. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation

Defaults By default, the isolate period is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the isolate period in the interface configuration mode.

```

Examples Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp icmp-guard isolate-period 180

```

Related Commands	Command	Description
	icmp-guard isolate-period	Sets the global isolate period.
	show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

18.75 nfpp icmp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

```

nfpp icmp-guard policy { per-src-ip | per-port } rate-limit-pps attack-threshold-pps
no nfpp icmp-guard policy { per-src-ip | per-port }
default nfpp icmp-guard policy { per-src-ip | per-port }

```

Parameter Description	Parameter	Description
	per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.

<code>attack-threshold-pps</code>	Sets the attack threshold, in range from 1 to 19,999.
-----------------------------------	---

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Interface configuration mode

Mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration The following example sets the rate-limit threshold and the attack threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp icmp-guard policy per-src-ip 5 10
Ruijie(config-if)# nfpp icmp-guard policy per-port 100 200
```

**Related
Commands**

Command	Description
<code>icmp-guard attack-threshold</code>	Sets the global attack threshold.
<code>icmp-guard rate-limit</code>	Sets the global rate-limit threshold.
<code>show nfpp icmp-guard summary</code>	Displays the configuration.
<code>show nfpp icmp-guard hosts</code>	Displays the monitored host.
<code>clear nfpp icmp-guard hosts</code>	Clears the isolated host.

Platform N/A

Description

18.76 nfpp ip-guard enable

Use this command to enable the IP anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard enable

no nfpp ip-guard enable

default nfpp ip-guard enable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults The IP anti-attack function is disabled on the interface.

Command Interface configuration mode

Mode

Usage Guide The interface IP anti-attack configuration is prior to the global configuration.

Configuration The following example enables the IP anti-attack function on the interface.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp ip-guard enable
```

Related Commands	Command	Description
		ip-guard enable
	show nfpp ip-guard summary	Displays the configuration.

Platform N/A

Description

18.77 nfpp ip-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard isolate-period { *seconds* | **permanent** }

no nfpp ip-guard isolate-period

default nfpp ip-guard isolate-period

Parameter Description	Parameter	Description
		<i>seconds</i>
	permanent	Permanent isolation

Defaults By default, the isolate period is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the isolate period in the interface configuration mode.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp ip-guard isolate-period 180
```

Related Commands	Command	Description
		ip-guard isolate-period
	show nfpp ip-guard summary	Displays the configuration.

Platform N/A

Description

18.78 nfpp ip-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard policy { **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp ip-guard policy { **per-src-ip** | **per-port** }

default nfpp ip-guard policy { **per-src-ip** | **per-port** }

Parameter Description	Parameter	Description
	per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from 1 to 19,999.

Defaults By default, the rate-limit threshold and the attack threshold are not configured.

Command Interface configuration mode

Mode

Usage Guide The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration The following example sets the rate-limit threshold and the attack threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp ip-guard policy per-src-ip 2 10
Ruijie(config-if)# nfpp ip-guard policy per-port 50 100
```

Related Commands	Command	Description
	ip-guard attack-threshold	Sets the global attack threshold.
	ip-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp ip-guard summary	Displays the configuration.
	show nfpp ip-guard hosts	Displays the monitored host.
	clear nfpp ip-guard hosts	Clears the isolated host.

Platform N/A

Description

18.79 nfpp ip-guard scan-threshold

Use this command to set the scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard scan-threshold *pkt-cnt*

no nfpp ip-guard scan-threshold

default nfpp ip-guard scan-threshold

Parameter Description	Parameter	Description
	<i>pkt-cnt</i>	Sets the scan threshold, in the range from 1 to 19,999.

Defaults By default, the sport-based scan threshold is not configured.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the scan threshold to 20pps.

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp ip-guard scan-threshold 20
```

Related Commands	Command	Description
	ip-guard attack-threshold	Sets the global attack threshold.
	show nfpp ip-guard summary	Displays the configuration.

Platform N/A

Description

18.80 nfpp nd-guard enable

Use this command to enable the ND anti-attack function on the interface.

Use the **no** or **default** form of this command to restore the default setting.

nfpp nd-guard enable

no nfpp nd-guard enable

default nfpp nd-guard enable

Parameter Description	Parameter	Description
	N/A	N/A

- Defaults** The ND anti-attack function is disabled on the interface.
- Command Mode** Interface configuration mode
- Usage Guide** The interface ND anti-attack configuration is prior to the global configuration.
- Configuration** The following example enables the ND anti-attack function on the interface.
- Examples**
- ```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp nd-guard enable
```

| Related Commands | Command                           | Description                          |
|------------------|-----------------------------------|--------------------------------------|
|                  | <b>nd-guard enable</b>            | Enables the ND anti-attack function. |
|                  | <b>show nfpp nd-guard summary</b> | Displays the configuration.          |

- Platform** N/A
- Description**

## 18.81 nfpp nd-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

Use the **no** or **default** form of this command to restore the default setting.

**nfpp nd-guard policy per-port { ns-na | rs | ra-redirect } rate-limit-pps attack-threshold-pps**

**no nfpp nd-guard policy per-port { ns-na | rs | ra-redirect }**

**default nfpp nd-guard policy per-port { ns-na | rs | ra-redirect }**

| Parameter Description       | Parameter                                                     | Description                                           |
|-----------------------------|---------------------------------------------------------------|-------------------------------------------------------|
|                             | <b>ns-na</b>                                                  | Sets the neighbor request and neighbor advertisement. |
| <b>rs</b>                   | Sets the router request.                                      |                                                       |
| <b>ra-redirect</b>          | Sets the router advertisement and the redirect packets.       |                                                       |
| <i>rate-limit-pps</i>       | Sets the rate-limit threshold, in the range from 1 to 19,999. |                                                       |
| <i>attack-threshold-pps</i> | Sets the attack threshold, in the range from 1 to 19,999.     |                                                       |

- Defaults** By default, the rate-limit threshold and the attack threshold are not configured.
- Command Mode** Interface configuration mode
- Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.
- Configuration** The following example sets the rate-limit threshold and the attack threshold.

**Examples**

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp nd-guard policy per-port ns-na 50 100
Ruijie(config-if)# nfpp nd-guard policy per-port rs 10 20
Ruijie(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

**Related Commands**

| Command                           | Description                           |
|-----------------------------------|---------------------------------------|
| <b>nd-guard attack-threshold</b>  | Sets the global attack threshold.     |
| <b>nd-guard rate-limit</b>        | Sets the global rate-limit threshold. |
| <b>show nfpp nd-guard summary</b> | Displays the configuration.           |

**Platform**

N/A

**Description**

## 18.82 no all-guard enable

Use this command to disable all NFPP guards (except guards self-defined and enabled in interface configuration mode).

**no all-guard enable**

Use this command to enable all NFPP guards.

**all-guard enable****Parameter**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Description****Command**

NFPP configuration mode

**Mode****Usage Guide**

- By default, all basic NFPP guards are enabled.
- This global command supports basic NFPP guards including ARP-GUARD, IP-GUARD, ICMP-GUARD, DHCP-GUARD, DHCPv6-GUARD and ND-GUARD.
- The **no** form command will disable all guards, which is displayed guard-by-guard by using the **show running-config** command. The exception is guards self-defined and configured in interface configuration mode.

**Configuration****Examples**

```
Ruijie(config)#show running-config | begin nfpp
nfpp
 log-buffer enable
 arp-guard rate-limit per-port 201
 arp-guard attack-threshold per-port 210
!
Ruijie(config)# nfpp
Ruijie(config-nfpp)#no all-guard enable
```



```

Ruijie(config-nfpp)#show running-config | begin nfpp
nfpp
 log-buffer enable
 no arp-guard enable
 arp-guard rate-limit per-port 201
 arp-guard attack-threshold per-port 210
 no icmp-guard enable
 no ip-guard enable
 no dhcp-guard enable
 no dhcpv6-guard enable
 no nd-guard enable
!
Ruijie(config-nfpp)#all-guard enable
Ruijie(config-nfpp)#show running-config | begin nfpp
nfpp
 log-buffer enable
 arp-guard rate-limit per-port 201
 arp-guard attack-threshold per-port 210
!
no service password-encryption
!

```

**Platform** N/A

**Description**

## 18.83 show nfpp arp-guard hosts

Use this command to display the monitored host.

**show nfpp arp-guard hosts** [ **statistics** | [[ **vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]] ]

| Parameter Description | Parameter           | Description                                                 |
|-----------------------|---------------------|-------------------------------------------------------------|
|                       | <b>statistics</b>   | Displays the statistical information of the monitored host. |
|                       | <i>vid</i>          | The VLAN ID                                                 |
|                       | <i>interface-id</i> | The interface name                                          |
|                       | <i>ip-address</i>   | The IP address                                              |
|                       | <i>mac-address</i>  | The MAC address                                             |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the statistical information of the monitored host.

```

Examples Ruijie# show nfpp arp-guard hosts statistics
success fail total
----- ---- -----
100 20 120

```

The following example shows the monitored host.

```

Ruijie# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN interface IP address MAC address remain-time(s)
---- -
1 Gi0/1 1.1.1.1 - 110
2 Gi0/2 1.1.2.1 - 61
*3 Gi0/3 - 0000.0000.1111 110
4 Gi0/4 - 0000.0000.2222 61
Total:4 hosts

```

**Related  
Commands**

| Command                           | Description                 |
|-----------------------------------|-----------------------------|
| <b>clear nfpp arp-guard hosts</b> | Clears the monitored hosts. |

**Platform** N/A

**Description**

## 18.84 show nfpp arp-guard scan

Use this command to display the ARP scan list.

```

show nfpp arp-guard scan [statistics | [[vlan vid] [interface interface-id] [ip-address]
[mac-address]]]

```

**Parameter  
Description**

| Parameter           | Description                                                |
|---------------------|------------------------------------------------------------|
| <b>statistics</b>   | Displays the statistical information of the ARP scan list. |
| <i>vid</i>          | The VLAN ID                                                |
| <i>interface-id</i> | The interface name                                         |
| <i>mac-address</i>  | The MAC address                                            |

**Defaults** N/A

**Command  
Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the ARP scan list.

```
Ruijie# show nfpp arp-guard scan statistics
arp-guard table has 4 record(s).
```

The following example displays the ARP scan list.

```
Ruijie# show nfpp arp-guard scan
VLAN interface IP address MAC address timestamp
---- -
1 Gi0/1 - 0000.0000.0001 2008-01-23 16:23:10
2 Gi0/2 1.1.1.1 0000.0000.0002 2008-01-23 16:24:10
3 Gi0/3 - 0000.0000.0003 2008-01-23 16:25:10
4 Gi0/4 - 0000.0000.0004 2008-01-23 16:26:10
Total:4 record(s)
```

The following example displays the ARP scan list.

```
Ruijie# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001
VLAN interface IP address MAC address timestamp
---- -
1 Gi0/1 - 0000.0000.0001 2008-01-23 16:23:10
Total:1 record(s)
```

**Related Commands**

| Command                              | Description                     |
|--------------------------------------|---------------------------------|
| <b>arp-guard scan-threshold</b>      | Sets the global scan threshold. |
| <b>nfpp arp-guard scan-threshold</b> | Sets the scan threshold.        |
| <b>clear nfpp arp-guard scan</b>     | Clears the ARP scan list.       |

**Platform** N/A

**Description**

### 18.85 show nfpp arp-guard summary

Use this command to display the configuration.

**show nfpp arp-guard summary**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration.

**Examples**

```
Ruijie# show nfpp arp-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global Enable 300 4/5/60 8/10/100 15
Gi 0/1 Enable 180 5/-/- 8/-/- -
Gi 0/2 Disable 200 4/5/60 8/10/100 20

Maximum count of monitored hosts: 1000
Monitor period:300s
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                                                                                                            |
| Status            | Enables/Disables the anti-attack function.                                                                                                                      |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold  | In the same format as the rate-limit.                                                                                                                           |
| Scan-threshold    | Scan threshold                                                                                                                                                  |

**Related Commands**

| Command                               | Description                                            |
|---------------------------------------|--------------------------------------------------------|
| <b>arp-guard attack-threshold</b>     | Sets the global attack threshold.                      |
| <b>arp-guard enable</b>               | Enables the anti-ARP attack function.                  |
| <b>arp-guard isolate-period</b>       | Sets the global isolate time.                          |
| <b>arp-guard monitor-period</b>       | Sets the monitor period.                               |
| <b>arp-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.        |
| <b>arp-guard rate-limit</b>           | Sets the global rate-limit threshold.                  |
| <b>arp-guard scan-threshold</b>       | Sets the global scan threshold.                        |
| <b>nfpp arp-guard enable</b>          | Enables the anti-ARP attack function on the interface. |
| <b>nfpp arp-guard isolate-period</b>  | Sets the isolate time.                                 |
| <b>nfpp arp-guard policy</b>          | Sets the rate-limit threshold and attack threshold.    |
| <b>nfpp arp-guard scan-threshold</b>  | Sets the scan threshold.                               |

**Platform** N/A  
**Description**

## 18.86 show nfpp define hosts

Use this command to display the monitored hosts.

```
show nfpp define hosts name [statistics | [[vlan vid] [interface interface-id] [ip-address] [mac-address] [ipv6-address]]]
```

| Parameter Description | Parameter           | Description                                 |
|-----------------------|---------------------|---------------------------------------------|
|                       | <i>name</i>         | Name of the user-defined anti-attack type   |
|                       | <b>statistics</b>   | Displays the statistics of monitored hosts. |
|                       | <i>vid</i>          | VLAN ID                                     |
|                       | <i>interface-id</i> | Interface name                              |
|                       | <i>ip-address</i>   | IP address                                  |
|                       | <i>mac-address</i>  | MAC address                                 |
|                       | <i>ipv6-address</i> | IPv6 address                                |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command allows filtering the hosts with parameters specified

**Configuration** The following example displays the monitored hosts.

```
Examples
Ruijie#show nfpp define hosts abc
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN interface MAC address remain-time(s)
 ---- -
*1 Gi4/2 00d0.f822.33e5 592
Total: 1 host
```

| Related Commands | Command                        | Description                                                  |
|------------------|--------------------------------|--------------------------------------------------------------|
|                  | <b>clear nfpp define hosts</b> | Clears the monitored hosts of user-defined anti-attack type. |

**Platform Description** N/A

## 18.87 show nfpp define summary

Use this command to display the configuration.

```
show nfpp define summary [name]
```

| Parameter Description | Parameter   | Description                               |
|-----------------------|-------------|-------------------------------------------|
|                       | <i>name</i> | Name of the user-defined anti-attack type |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the configuration. Without the name specified, all user-defined anti-attack types will be displayed.

**Configuration** The following example displays the configuration.

**Examples**

```
Ruijie#show nfpp define summary abc
Define abc summary:
match etype 0x800 src-ip 1.1.1.1 src-ip-mask 255.255.255.255
Maximum count of monitored hosts: 20000
Monitor period:600s
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Rate-limit Attack-threshold
Global Disable -/10/- -/20/-
Gi4/1 Enable -/-/- -/-/-
```

| Field            | Description                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface        | If the interface field is displayed as Global, it means that is configured in the global configuration mode.                                                    |
| Status           | Enables/ Disables the anti-attack function.                                                                                                                     |
| Rate-limit       | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit.                                                                                                                           |

**Related Commands**

| Command                     | Description                                                  |
|-----------------------------|--------------------------------------------------------------|
| <b>match</b>                | Clears the monitored hosts of user-defined anti-attack type. |
| <b>policy</b>               | Attack threshold and rate-limit threshold.                   |
| <b>isolate-period</b>       | Isolates time                                                |
| <b>monitored-period</b>     | Monitored time                                               |
| <b>monitored-host-limit</b> | Maximum monitored host number                                |

**Platform Description** N/A

## 18.88 show nfpp define trusted-host

Use this command to display the trusted host free from monitoring.

**show nfpp define trusted-host** *name*

| Parameter Description | Parameter   | Description                               |
|-----------------------|-------------|-------------------------------------------|
|                       | <i>name</i> | Name of the user-defined anti-attack type |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the trusted host configuration.

**Examples**

```
Ruijie# show nfpp define trusted-host tcp
Define tcp:
IP address mask
----- -
1.1.1.0 255.255.255.0
1.1.2.0 255.255.255.0
Total:2 record(s)
```

| Related Commands | Command             | Description                   |
|------------------|---------------------|-------------------------------|
|                  | <b>trusted-host</b> | Configures the trusted hosts. |

**Platform** N/A

**Description**

## 18.89 show nfpp dhcp-guard hosts

Use this command to display the monitored host.

**show nfpp dhcp-guard hosts** [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

| Parameter Description | Parameter           | Description                                                 |
|-----------------------|---------------------|-------------------------------------------------------------|
|                       | <b>statistics</b>   | Displays the statistical information of the monitored host. |
|                       | <i>vid</i>          | VLAN ID                                                     |
|                       | <i>interface-id</i> | Interface name                                              |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the monitored host.

**Examples**

```
Ruijie# show nfpp dhcp-guard hosts statistics
success fail total
----- ---- -----
100 20 120
```

The following example displays the monitored host.

```
Ruijie# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN interface MAC address remain-time(seconds)
---- -
1 gi0/2 0000.0000.0001 10
*2 gi0/1 0000.0000.0002 20
Total:2 host(s)
```

**Related Commands**

| Command                            | Description                |
|------------------------------------|----------------------------|
| <b>clear nfpp dhcp-guard hosts</b> | Clears the monitored host. |

**Platform** N/A

**Description**

## 18.90 show nfpp dhcp-guard summary

Use this command to display the configuration.

**show nfpp dhcp-guard summary**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A



**Configuration** The following example displays the configuration.

**Examples**

```
Ruijie# show nfpp dhcp-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold
Global Enable 300 -/5/150 -/10/300
Gi 0/1 Enable 180 -/6/- -/8/-
Gi 0/2 Disable 200 -/5/30 -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                                                                                                            |
| Status            | Enables/Disables the anti-attack function.                                                                                                                      |
| Isolate-period    | Isolate period                                                                                                                                                  |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold  | In the same format as the rate-limit.                                                                                                                           |

**Related  
Commands**

| Command                                | Description                                             |
|----------------------------------------|---------------------------------------------------------|
| <b>dhcp-guard attack-threshold</b>     | Sets the global attack threshold.                       |
| <b>dhcp-guard enable</b>               | Enables the DHCP anti-attack function.                  |
| <b>dhcp-guard isolate-period</b>       | Sets the global isolate time.                           |
| <b>dhcp-guard monitor-period</b>       | Sets the monitor period.                                |
| <b>dhcp-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.         |
| <b>dhcp-guard rate-limit</b>           | Sets the global rate-limit threshold.                   |
| <b>nfpp dhcp-guard enable</b>          | Enables the DHCP anti-attack function on the interface. |
| <b>nfpp dhcp-guard isolate-period</b>  | Sets the isolate time.                                  |
| <b>nfpp dhcp-guard policy</b>          | Sets the rate-limit threshold and attack threshold.     |

**Platform** N/A

**Description**

## 18.91 show nfpp dhcpv6-guard hosts

Use this command to display the monitored host.

**show nfpp dhcpv6-guard hosts** [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

| Parameter Description | Parameter           | Description                                                 |
|-----------------------|---------------------|-------------------------------------------------------------|
|                       | <b>statistics</b>   | Displays the statistical information of the monitored host. |
|                       | <i>vid</i>          | The VLAN ID                                                 |
|                       | <i>interface-id</i> | The interface name                                          |
|                       | <i>mac-address</i>  | The MAC address                                             |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the monitored host.

**Examples**

```
Ruijie# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN interface MAC address remain-time(seconds)

*1 gi0/2 0000.0000.0001 10
*2 gi0/1 0000.0000.0002 20
Total:2 host(s)
```

| Related Commands | Command                              | Description                |
|------------------|--------------------------------------|----------------------------|
|                  | <b>clear nfpp dhcpv6-guard hosts</b> | Clears the monitored host. |

**Platform Description** N/A

## 18.92 show nfpp dhcpv6-guard summary

Use this command to display the configuration.

**show nfpp dhcpv6-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode****Usage Guide** N/A**Configuration** The following example displays the configuration.**Examples**

```
Ruijie#show nfpp dhcpv6-guard summary
```

```
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
```

```
Interface Status Rate-limit Attack-threshold
Global Enable -/5/1200 -/10/1500
```

```
Maximum count of monitored hosts: 20000
```

```
Monitor period: 600s
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                                                                                                            |
| Status            | Enables/Disables the anti-attack function.                                                                                                                      |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold  | In the same format as the rate-limit.                                                                                                                           |

**Related Commands**

| Command                                  | Description                                               |
|------------------------------------------|-----------------------------------------------------------|
| <b>dhcpv6-guard attack-threshold</b>     | Sets the global attack threshold.                         |
| <b>dhcpv6-guard enable</b>               | Enables the DHCPv6 anti-attack function.                  |
| <b>dhcpv6-guard monitor-period</b>       | Sets the monitor period.                                  |
| <b>dhcpv6-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.           |
| <b>dhcpv6-guard rate-limit</b>           | Sets the global rate-limit threshold.                     |
| <b>nfpp dhcpv6-guard enable</b>          | Enables the DHCPv6 anti-attack function on the interface. |
| <b>nfpp dhcpv6-guard policy</b>          | Sets the rate-limit threshold and attack threshold.       |

**Platform** N/A**Description**

## 18.93 show nfpp fw-guard hosts

Use this command to display the FW-guard monitored host.

```
show nfpp fw-guard hosts [statistics | [[vlan vid] [ip-address]]]
```

| Parameter Description | Parameter         | Description                                                 |
|-----------------------|-------------------|-------------------------------------------------------------|
|                       | <b>statistics</b> | Displays the statistical information of the monitored host. |
|                       | <i>vid</i>        | The VLAN ID                                                 |
|                       | <i>ip-address</i> | The IP address                                              |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays statistics of FW-guard monitored hosts.

**Examples**

```
Ruijie# show nfpp fw-guard hosts statistics
success fail total
----- ---- -----
100 20 120
```

The following example displays the FW-guard monitored host.

```
Ruijie# show nfpp fw-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
VLAN interface IP address remain-time(s)
---- - - -
*301 - 10.32.0.3 585
Total: 1 host
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 18.94 show nfpp fw-guard summary

Use this command to display the FW-guard configuration.

**show nfpp fw-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the FW-guard configuration.

**Examples**

```
Ruijie# show nfpp fw-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Rate-limit Attack-threshold
Global Enable 50/-- 100/--

Maximum count of monitored hosts: 20000
Monitor period: 600s
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                                                                                                            |
| Status            | Enables/Disables FW-guard function.                                                                                                                             |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold  | In the same format as the rate-limit.                                                                                                                           |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 18.95 show nfpp icmp-guard trusted-host

Use this command to display the trusted host free from being monitored.

**show nfpp icmp-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the trusted host free from being monitored.

```

Examples Ruijie# show nfpp icmp-guard trusted-host
IP address mask

1.1.1.0 255.255.255.0
1.1.2.0 255.255.255.0
Total:2 record(s)

```

**Related  
Commands**

| Command                        | Description            |
|--------------------------------|------------------------|
| <b>icmp-guard trusted-host</b> | Sets the trusted host. |

**Platform** N/A  
**Description**

## 18.96 show nfpp ip-guard hosts

Use this command to display the monitored host.

**show nfpp ip-guard hosts** [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

**Parameter  
Description**

| Parameter           | Description                                                 |
|---------------------|-------------------------------------------------------------|
| <b>statistics</b>   | Displays the statistical information of the monitored host. |
| <i>vid</i>          | The VLAN ID.                                                |
| <i>interface-id</i> | The interface name.                                         |
| <i>mac-address</i>  | The MAC address.                                            |

**Defaults** N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the monitored host.

```

Examples Ruijie# show nfpp ip-guard hosts statistics
success fail total

100 20 120

```

The following example displays the monitored host.

```
Ruijie#show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN interface IP address Reason remain-time(s)
---- -
1 Gi0/1 1.1.1.1 ATTACK 110
2 Gi0/2 1.1.2.1 SCAN 61
Total:2 host(s)
```

**Related  
Commands**

| Command                          | Description                |
|----------------------------------|----------------------------|
| <b>clear nfpp ip-guard hosts</b> | Clears the monitored host. |

**Platform** N/A

**Description**

## 18.97 show nfpp ip-guard summary

Use this command to display the configuration.

**show nfpp ip-guard summary**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command  
Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration.

**Examples**

```
Ruijie# show nfpp ip-guard summary
(format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global Enable 300 4/-/60 8/-/100 15
Gi 0/1 Enable 180 5/-/- 8/-/- -
Gi 0/2 Disable 200 4/-/60 8/-/100 20

Maximum count of monitored hosts: 1000
Monitor period..300s
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                                                                                                            |
| Status            | Enables/Disables the anti-attack function.                                                                                                                      |
| Isolate-period    | Isolate period                                                                                                                                                  |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold  | In the same format as the rate-limit.                                                                                                                           |
| Scan-threshold    | Scan threshold                                                                                                                                                  |

#### Related Commands

| Command                              | Description                                           |
|--------------------------------------|-------------------------------------------------------|
| <b>ip-guard attack-threshold</b>     | Sets the global attack threshold.                     |
| <b>ip-guard enable</b>               | Enables the IP anti-attack function.                  |
| <b>ip-guard isolate-period</b>       | Sets the global isolate time.                         |
| <b>ip-guard monitor-period</b>       | Sets the monitor period.                              |
| <b>ip-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.       |
| <b>ip-guard rate-limit</b>           | Sets the global rate-limit threshold.                 |
| <b>nfpp ip-guard enable</b>          | Enables the IP anti-attack function on the interface. |
| <b>nfpp ip-guard isolate-period</b>  | Sets the isolate time.                                |
| <b>nfpp ip-guard policy</b>          | Sets the rate-limit threshold and attack threshold.   |

**Platform** N/A

**Description**

## 18.98 show nfpp ip-guard trusted-host

Use this command to display the trusted host free from being monitored.

**show nfpp ip-guard trusted-host**

#### Parameter Description

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A



**Configuration** The following example displays the trusted host free from being monitored.

**Examples**

```
Ruijie# show nfpp ip-guard trusted-host
IP address mask

1.1.1.0 255.255.255.0
1.1.2.0 255.255.255.0
Total.2 record(s)
```

| Related Commands | Command | Description                  |
|------------------|---------|------------------------------|
|                  |         | <b>ip-guard trusted-host</b> |

**Platform** N/A

**Description**

## 18.99 show nfpp log

Use this command to display the NFPP log configuration.

**show nfpp log summary**

Use this command to display the NFPP log buffer area content.

**show nfpp log buffer [ statistics ]**

| Parameter Description | Parameter | Description       |
|-----------------------|-----------|-------------------|
|                       |           | <b>statistics</b> |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** When the log buffer area is full, the subsequent logs are to be dropped, and an entry with all attributes "-" is displayed in the log buffer area. The administrator shall increase the capacity of the log buffer area or improve the rate of generating the syslog.

The generated syslog in the log buffer area carries with the timestamp, for example:

```
%NFPP_ARP_GUARD-4-DOS_DETECTED:
```

```
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)
```

**Configuration** The following example displays the NFPP log configuration.

**Examples**

```
Ruijie#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
Logging:
```

```
VLAN 1-3, 5
interface Gi 0/1
interface Gi 0/2
```

The following example displays the log number in the buffer area.

```
Ruijie#show nfpp log buffer statistics
```

There are 6 logs in buffer.

The following example shows the NFPP log buffer area:

```
Ruijie#show nfpp log buffer
```

| Protocol | VLAN | Interface | IP address | MAC address    | Reason         | Timestamp              |
|----------|------|-----------|------------|----------------|----------------|------------------------|
| ARP      | 1    | Gi0/1     | 1.1.1.1    | -              | DoS            | 2009-05-30<br>16:23:10 |
| ARP      | 1    | Gi0/1     | 1.1.1.1    | -              | ISOLATED       | 2009-05-30<br>16:23:10 |
| ARP      | 1    | Gi0/1     | 1.1.1.2    | -              | DoS            | 2009-05-30<br>16:23:15 |
| ARP      | 1    | Gi0/1     | 1.1.1.2    | -              | ISOLATE_FAILED | 2009-05-30<br>16:23:15 |
| ARP      | 1    | Gi0/1     | -          | 0000.0000.0001 | SCAN           | 2009-05-30<br>16:30:10 |
| ARP      | -    | Gi0/2     | -          | -              | PORT_ATTACKED  | 2009-05-30<br>16:30:10 |

| Field    | Description                                        |
|----------|----------------------------------------------------|
| Protocol | ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT |
| Reason   | DoS, ISOLATED, ISOLATE_FAILE, SCAN, PORT_ATTACKED  |

#### Related Commands

| Command               | Description                      |
|-----------------------|----------------------------------|
| <b>clear nfpp log</b> | Clears the NFPP log buffer area. |

#### Platform Description

N/A

## 18.100 show nfpp nd-guard hosts

Use this command to display the monitored host.

```
show nfpp nd-guard hosts [statistics | [[vlan vid] [interface interface-id]]]
```

#### Parameter Description

| Parameter         | Description                                    |
|-------------------|------------------------------------------------|
| <b>statistics</b> | Displays the statistics of the monitored host. |

|                     |                                     |
|---------------------|-------------------------------------|
| <i>vid</i>          | Sets the VLAN ID.                   |
| <i>interface-id</i> | Sets the interface name and number. |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the statistics of the host monitored by ND-guard.

**Examples**

```
Ruijie#show nfpp nd-guard hosts statistics
success fail total
----- -
10 2 12
```

The following example displays the host monitored by ND-guard. The “remain-time(s)” refers to the remaining time of isolation.

```
Ruijie#show nfpp nd-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
VLAN interface ND-guard remain-time(s)
---- -
- Gi4/2 ns-na-guard 174
- Gi4/2 rs-guard 98
- Gi4/2 ra-redirect-guard 127
Total: 3 hosts
```

**Platform** N/A

**Description**

## 18.101 show nfpp nd-guard summary

Use this command to display the configuration.

**show nfpp nd-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration.

**Examples**

```
Ruijie# show nfpp nd-guard summary
(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface Status Rate-limit Attack-threshold
Global Enable 20/5/10 40/10/20
Gi 0/1 Enable 15/15/15 30/30/30
Gi 0/2 Disable -/5/30 -/10/50
```

| Field             | Description                                                             |
|-------------------|-------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                    |
| Status            | Enables/Disables the anti-attack function.                              |
| Rate-limit        | In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT. |
| Attack-threshold  | In the same format as the rate-limit.                                   |

**Related Commands**

| Command                          | Description                                           |
|----------------------------------|-------------------------------------------------------|
| <b>nd-guard attack-threshold</b> | Sets the global attack threshold.                     |
| <b>nd-guard enable</b>           | Enables the ND anti-attack function.                  |
| <b>nd-guard rate-limit</b>       | Sets the global rate-limit threshold.                 |
| <b>nfpp nd-guard enable</b>      | Enables the ND anti-attack function on the interface. |
| <b>nfpp nd-guard policy</b>      | Sets the rate-limit threshold and attack threshold.   |

**Platform** N/A

**Description**

**18.102 trusted-host**

Use this command to set the trusted hosts free form monitoring.

Use the **no** or **default** form of this command to restore the default setting,

**trusted-host** { *mac mac\_mask* | *ip mask* | *IPv6/prefixlen* }

**no trusted-host** { **all** | *mac mac\_mask* | *ip mask* | *IPv6/prefixlen* }

**default trusted-host**

**Parameter Description**

| Parameter             | Description                                                             |
|-----------------------|-------------------------------------------------------------------------|
| <i>ip</i>             | Sets the IP address                                                     |
| <i>mac</i>            | MAC address                                                             |
| <i>mac_mask</i>       | MAC address mask                                                        |
| <i>IPv6/prefixlen</i> | IPv6 address and mask length                                            |
| <i>mask</i>           | IP mask                                                                 |
| <b>all</b>            | Deletes the configuration of all trusted hosts with the no form of this |

|  |          |
|--|----------|
|  | command. |
|--|----------|

**Defaults** N/A

**Command Mode** NFPP define configuration mode

**Usage Guide** The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to be sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.

Before configuring the trusted-host, the match type must be configured. If the message type configured by the match is Ipv4, the Ipv6 trusted addresses are not allowed. In the same way, if the message type is IPv6, the IPv4 trusted addresses are not allowed.

**Configuration** The following example sets the trusted hosts free form monitoring.

**Examples**

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
Ruijie(config-nfpp-define)#trusted-host 1.1.1.1 255.255.255.255
```

**Related Commands**

| Command                              | Description                              |
|--------------------------------------|------------------------------------------|
| <b>show nfpp define trusted-host</b> | Displays the trusted host configuration. |

**Platform Description** N/A

## 19 DoS Protection Commands

### 19.1 ip deny invalid-l4port

Use this command to enable the anti-attack of the self-consumption.

Use the **no** form of this command to restore the default setting.

**ip deny invalid-l4port**

**no ip deny invalid-l4port**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enables the anti-attack of the self-consumption.

**Examples** Ruijie(config)# ip deny invalid-l4port

The following example disables the anti-attack of the self-consumption.

Ruijie(config)# no ip deny invalid-l4port

| Related Commands | Command                            | Description                                                |
|------------------|------------------------------------|------------------------------------------------------------|
|                  | <b>show ip deny invalid-l4port</b> | Displays the state of anti-attack of the self-consumption. |

**Platform** N/A

**Description**

### 19.2 ip deny invalid-tcp

Use this command to enable the anti-attack of the invalid TCP packets.

Use the **no** form of this command to restore the default setting.

**ip deny invalid-tcp**

**no ip deny invalid-tcp**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |     |     |
|--------------------|-----|-----|
| <b>Description</b> |     |     |
|                    | N/A | N/A |

**Defaults** The function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example enables the anti-attack of the invalid TCP packets:

**Examples**

```
Ruijie(config)# ip deny invalid-tcp
```

The following example disables the anti-attack of the invalid TCP packets:

```
Ruijie(config)# no ip deny invalid-tcp
```

| <b>Related Commands</b> | Command                         | Description                                                   |
|-------------------------|---------------------------------|---------------------------------------------------------------|
|                         | <b>show ip deny invalid-tcp</b> | Displays the state of anti-attack of the invalid TCP packets. |

**Platform** N/A

**Description**

## 19.3 ip deny land

Use this command to enable the anti-land-attack.

Use the **no** form of this command to restore the default setting.

**ip deny land**

**no ip deny land**

| <b>Parameter Description</b> | Parameter | Description |
|------------------------------|-----------|-------------|
|                              | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example enables the anti-land-attack:

**Examples**

```
Ruijie(config)# ip deny land
```

The following example disables the anti-land-attack:

```
Ruijie(config)# no ip deny land
```

**Related  
Commands**

| Command           | Description                          |
|-------------------|--------------------------------------|
| show ip deny land | Displays the anti-land-attack state. |

**Platform** N/A**Description**

## 19.4 show ip deny

Use this command to display the state of the anti-DOS-attack.

**show ip deny**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A**Command  
Mode** Privileged EXEC mode**Usage Guide** N/A**Configuration** The following example displays the state of the anti-DOS-attack.**Examples**

```
ruijie#show ip deny
 Protect against Land attack On
 Protect against invalid L4port attack Off
 Protect against invalid TCP attack Off
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A**Description**

## 19.5 show ip deny invalid-l4port

Use this command to display the state of the anti-consumption-attack.

**show ip deny invalid-l4port**



| <b>Parameter Description</b>  | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>                                                              | Parameter | Description | N/A | N/A |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|-----|-----|
| Parameter                     | Description                                                                                                                                                                                                        |           |             |     |     |
| N/A                           | N/A                                                                                                                                                                                                                |           |             |     |     |
| <b>Defaults</b>               | N/A                                                                                                                                                                                                                |           |             |     |     |
| <b>Command Mode</b>           | Privileged EXEC mode                                                                                                                                                                                               |           |             |     |     |
| <b>Usage Guide</b>            | N/A                                                                                                                                                                                                                |           |             |     |     |
| <b>Configuration Examples</b> | <p>The following example displays the state of the anti-consumption-attack.</p> <pre>Ruijie# show ip deny invalid-l4port DoS Protection Mode           State ----- protect against invalid l4port attack Off</pre> |           |             |     |     |
| <b>Related Commands</b>       | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>                                                                | Command   | Description | N/A | N/A |
| Command                       | Description                                                                                                                                                                                                        |           |             |     |     |
| N/A                           | N/A                                                                                                                                                                                                                |           |             |     |     |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                                |           |             |     |     |

## 19.6 show ip deny invalid-tcp

Use this command to display the state of the anti-attack of the invalid TCP packets.

**show ip deny invalid-tcp**

| <b>Parameter Description</b>  | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>                                | Parameter | Description | N/A | N/A |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|-----|-----|
| Parameter                     | Description                                                                                                                                                                          |           |             |     |     |
| N/A                           | N/A                                                                                                                                                                                  |           |             |     |     |
| <b>Defaults</b>               | N/A                                                                                                                                                                                  |           |             |     |     |
| <b>Command Mode</b>           | Privileged EXEC mode                                                                                                                                                                 |           |             |     |     |
| <b>Usage Guide</b>            | N/A                                                                                                                                                                                  |           |             |     |     |
| <b>Configuration Examples</b> | <p>The following example displays the state of the anti-attack of the invalid TCP packets.</p> <pre>Ruijie# show ip deny invalid-tcp DoS Protection Mode           State -----</pre> |           |             |     |     |

```
protect against invalid tcp attack On
```

**Related Commands**

| Command                    | Description                                         |
|----------------------------|-----------------------------------------------------|
| <b>ip deny invalid-tcp</b> | Enables the anti-attack of the invalid TCP packets. |

**Platform** N/A**Description**

## 19.7 show ip deny land

Use this command to display the anti-land-attack state.

```
show ip deny land
```

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A**Command Mode** Privileged EXEC mode**Usage Guide** N/A**Configuration** The following example displays the anti-land-attack state.**Examples**

```
Ruijie# show ip deny land
DoS Protection Mode State

protect against land attack On
```

**Related Commands**

| Command                | Description                            |
|------------------------|----------------------------------------|
| <b>no ip deny land</b> | Enables the anti-land-attack function. |

**Platform** N/A**Description**



## ACL & QoS Commands

---

1. ACL Commands
2. QoS Commands

# 1 ACL Commands

## 1.1 command ID table

| ID                   | Meaning                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID                   | Number of access list. Range:<br>Standard IP ACL: 1 to 99, 1300 to 1999<br>Extended IP ACL: 100 to 199,2000 to 2699<br>Extended MAC ACL: 700 to 799<br>Extended expert ACL: 2700 to 2899                                                                                                                                                                           |
| name                 | ACL name                                                                                                                                                                                                                                                                                                                                                           |
| sn                   | ACL SN (products can be set according to the priority)                                                                                                                                                                                                                                                                                                             |
| start-sn             | Start sequence number                                                                                                                                                                                                                                                                                                                                              |
| inc-sn               | Sequence number increment                                                                                                                                                                                                                                                                                                                                          |
| deny                 | If matched, access is denied.                                                                                                                                                                                                                                                                                                                                      |
| permit               | If matched, access is permitted.                                                                                                                                                                                                                                                                                                                                   |
| port                 | Protocol number. For IPv6, this field can be IPv6, ICMP, TCP, UDP and numbers 0 to 255. For IPv4, it can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP,AHP, ESP, PCP, PIM and IP, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as ICMP, TCP and UDP, are listed individually. |
| interface <i>idx</i> | Interface index                                                                                                                                                                                                                                                                                                                                                    |
| src                  | Packet source IP address (host address or network address)                                                                                                                                                                                                                                                                                                         |
| src-wildcard         | Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.                                                                                                                                                                                                                                                                                      |
| src-ipv6-pfix        | Source IPv6 network address or network type                                                                                                                                                                                                                                                                                                                        |
| dst-ipv6-pfix        | Destination IPv6 network address or network type                                                                                                                                                                                                                                                                                                                   |
| pfix-len             | Prefix mask length                                                                                                                                                                                                                                                                                                                                                 |
| src-ipv6-addr        | Source IPv6 address                                                                                                                                                                                                                                                                                                                                                |
| dst-ipv6-addr        | Destination IPv6 address                                                                                                                                                                                                                                                                                                                                           |
| dscp                 | Differential service code point, and code point value. Range: 0 to 63                                                                                                                                                                                                                                                                                              |
| flow-label           | Flow label in the range 0 to 1048575                                                                                                                                                                                                                                                                                                                               |
| dst                  | Packet destination IP address (host address or network address)                                                                                                                                                                                                                                                                                                    |
| dst-wildcard         | Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32                                                                                                                                                                                                                                                                                       |
| fragment             | Packet fragment filtering.                                                                                                                                                                                                                                                                                                                                         |

|                                 |                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| precedence                      | Packet precedence value (0 to 7)                                                                                                                                                                         |
| range                           | The layer 4 port number range of the packet.                                                                                                                                                             |
| time-range<br>tm-rng-name       | Time range of packet filtering, named <i>tm-rng-name</i>                                                                                                                                                 |
| tos                             | Type of service (0 to 15)                                                                                                                                                                                |
| cos                             | Class of service (0-7)                                                                                                                                                                                   |
| cos inner <i>cos</i>            | COS of the packet tag                                                                                                                                                                                    |
| icmp-type                       | ICMP message type (0 to 255)                                                                                                                                                                             |
| icmp-code                       | ICMP message type code (0 to 255)                                                                                                                                                                        |
| icmp-message                    | ICMP message type name (0 to 255)                                                                                                                                                                        |
| operator port[port]             | Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)<br><i>port</i> indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number |
| src-mac-addr                    | Physical address of the source host                                                                                                                                                                      |
| dst-mac-addr                    | Physical address of the destination host                                                                                                                                                                 |
| VID vid                         | VLAN ID                                                                                                                                                                                                  |
| VID inner vid                   | VID of the tag                                                                                                                                                                                           |
| ethernet-type                   | Ethernet protocol type. 0x value can be entered.                                                                                                                                                         |
| match-all <i>tcpf</i>           | Match all bits of the TCP flag.                                                                                                                                                                          |
| established                     | Match the RST or ACK bit of the TCP flag.                                                                                                                                                                |
| <i>text</i>                     | Remark text                                                                                                                                                                                              |
| <i>in</i>                       | Filter the incoming packets of the interface                                                                                                                                                             |
| <i>out</i>                      | Filter the outgoing packets of the interface                                                                                                                                                             |
| {rule mask offset} <sup>+</sup> | rule: Hexadecimal value field; mask: Hexadecimal mask field<br>offset: Refer to the offset table<br>“+” sign indicates at least one group                                                                |
| log                             | Output the matching syslog when the packet matches the ACL rule.                                                                                                                                         |

| Letter | Meaning                                       | Offset | Letter | Meaning                | Offset |
|--------|-----------------------------------------------|--------|--------|------------------------|--------|
| A      | Destination MAC                               | 0      | O      | TTL field              | 34     |
| B      | Source MAC                                    | 6      | P      | Protocol number        | 35     |
| C      | Data frame length field                       | 12     | Q      | IP check sum           | 36     |
| D      | VLAN tag field                                | 14     | R      | Source IP address      | 38     |
| E      | DSAP (Destination Service Access Point) field | 18     | S      | Destination IP address | 42     |

|   |                                          |    |    |                                    |    |
|---|------------------------------------------|----|----|------------------------------------|----|
| F | SSAP (Source Service Access Point) field | 19 | T  | TCP source port                    | 46 |
| G | Ctrl field                               | 20 | U  | TCP destination port               | 48 |
| H | Org Code field                           | 21 | V  | Sequence number                    | 50 |
| I | Encapsulated data type                   | 24 | W  | Confirmation field                 | 54 |
| J | IP version number                        | 26 | XY | IP header length and reserved bits | 58 |
| K | TOS field                                | 27 | Z  | Reserved bits and flags bit        | 59 |
| L | Length of IP packet                      | 28 | a  | Windows size field                 | 60 |
| M | ID                                       | 30 | b  | Others                             | 62 |
| N | Flags field                              | 32 |    |                                    |    |

The offsets of fields in the above table are their offsets in 802.3 data frames of SNAP+tag.

## 1.2 access-list

Use this command to create an access list to filter data packets. Use the **no** form of this command to remove the specified access list.

- Standard IP access list (1 to 99, 1300 to 1999)

```
access-list id { deny | permit } { source source-wildcard | host source | any | interface idx }
[time-range tm-range-name] [log]
```

- Extended IP access list (100 to 199, 2000 to 2699)

```
access-list id {deny | permit} protocol {source source-wildcard | host source | any} interface idx }
{destination destination-wildcard | host destination | any} [precedence precedence] [tos tos]
[fragment] [range lower upper] [time-range time-range-name] [log]
```

- Extended MAC access list (700 to 799)

```
access-list id {deny | permit} {any | host source-mac-address | source-mac-address mask } {any |
host destination-mac-address | destination-mac-address mask } [ethernet-type][cos [out][inner in]]
```

- Extended expert access list (2700 to 2899)

```
access-list id {deny | permit} [protocol] [ethernet-type][cos [out][inner in]] [VID [out][inner in]]
{source source-wildcard | host source | any} {host source-mac-address | any} {destination
destination-wildcard | host destination | any} {host destination-mac-address | any} [[precedence
precedence] [tos tos] [fragment] [time-range time-range-name]
```

- When you select the Ethernet-type field or cos field:

```
access-list id {deny | permit} [ethernet-type]/cos [out][inner in]] [VID [out][inner in]] {source
source-wildcard | host source | any} {host source-mac-address | any} {destination
destination-wildcard | host destination | any} {host destination-mac-address | any} [time-range
time-range-name]
```

- When you select the protocol field:

```
access-list id {deny | permit} protocol [VID [out][inner in]] {source source-wildcard | host source |
any} {host source-mac-address | any} {destination destination-wildcard | host destination | any}
{host destination-mac-address | any} [precedence precedence] [tos tos] [fragment] [range lower
upper] [time-range time-range-name]
```

- Extended expert ACLs of some important protocols:

**Internet Control Message Protocol (ICMP)**

```
access-list id {deny | permit} icmp [VID [out][inner in]] {source source-wildcard | host source | any}
{host source-mac-address | any} {destination destination-wildcard | host destination | any} {host
destination-mac-address | any} [icmp-type] [[icmp-type [icmp-code]]] [icmp-message]]
[precedence precedence] [tos tos] [fragment] [time-range time-range-name]
```

**Transmission Control Protocol (TCP)**

```
access-list id {deny | permit} tcp [VID [out][inner in]]{source source-wildcard | host Source | any}
{host source-mac-address | any } [operator port [port]] {destination destination-wildcard | host
destination | any} {host destination-mac-address | any} [operator port [port]] [precedence
precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [match-all
tcp-flag | established]
```

**User Datagram Protocol (UDP)**

```
access-list id {deny | permit} udp [VID [out][inner in]] {source source-wildcard | host source |
any} {host source-mac-address | any } [operator port [port]] {destination destination-wildcard |
host destination | any}{host destination-mac-address | any} [operator port [port]] [precedence
precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]
```

Parameter  
Description

| Parameter            | Description                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id                   | Access list number. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.                                                                                                                            |
| deny                 | If not matched, access is denied.                                                                                                                                                                                                                      |
| permit               | If matched, access is permitted.                                                                                                                                                                                                                       |
| source               | Specify the source IP address (host address or network address).                                                                                                                                                                                       |
| source-wildcard      | It can be discontinuous, for example, 0.255.0.32.                                                                                                                                                                                                      |
| protocol             | IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately. |
| destination          | Specify the destination IP address (host address or network address).                                                                                                                                                                                  |
| destination-wildcard | Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.                                                                                                                                                              |
| fragment             | Packet fragment filtering                                                                                                                                                                                                                              |
| precedence           | Specify the packet priority.                                                                                                                                                                                                                           |
| precedence           | Packet precedence value (0 to 7)                                                                                                                                                                                                                       |
| range                | Layer4 port number range of the packet.                                                                                                                                                                                                                |
| lower                | Lower limit of the layer4 port number.                                                                                                                                                                                                                 |
| upper                | Upper limit of the layer4 port number.                                                                                                                                                                                                                 |
| time-range           | Time range of packet filtering                                                                                                                                                                                                                         |

|                              |                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------|
| time-range-name              | Time range name of packet filtering                                                         |
| tos                          | Specify type of service.                                                                    |
| tos                          | ToS value (0 to 15)                                                                         |
| icmp-type                    | ICMP message type (0 to 255)                                                                |
| icmp-code                    | ICMP message type code (0 to 255)                                                           |
| icmp-message                 | ICMP message type name                                                                      |
| operator                     | Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)                       |
| port [ port ]                | Port number; range needs two port numbers, while other operators only need one port number. |
| host source-mac-address      | Source physical address                                                                     |
| host destination-mac-address | Destination physical address                                                                |
| VID vid                      | Match the specified VID.                                                                    |
| ethernet-type                | Ethernet type                                                                               |
| match-all                    | Match all the bits of the TCP flag.                                                         |
| tcp-flag                     | Match the TCP flag.                                                                         |
| established                  | Match the RST or ACK bits, not other bits of the TCP flag.                                  |

**Defaults** N/A

**Command** Global configuration mode.

**Mode**

**Usage Guide** To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs:  
The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses.  
The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses.

The extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.

The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID.

For the layer-3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence*/**tos** *tos*/**fragments**/**range** *lower upper*/**time-range** *time-range-name*

The TCP Flag includes part or all of the following:

- urg
- ack
- psh
- rst
- syn
- fin

The packet precedence is as below:



- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service types are as below:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The ICMP message types are as below:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big

- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- device-advertisement
- device-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The TCP ports are as follows. A port can be specified by port name and port number:

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- ldp
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk

- telnet
- time
- uucp
- whois
- www

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

The Ethernet types are as below:

- aarp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console

- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

**Configuration** 1. Example of the standard IP ACL

**Examples** The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
Ruijie (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
Ruijie (config)#access-list 102 permit tcp any any eq domain log
Ruijie (config)#access-list 102 permit udp any any eq domain log
Ruijie (config)#access-list 102 permit icmp any any echo log
Ruijie (config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below:

```
Ruijie (config)#access-list 702 deny host 00d0f8000c0c any aarp
Ruijie (config)# interface gigabitethernet 1/1
Ruijie (config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Ruijie (config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044
any any
Ruijie (config)# access-list 2702 permit any any any any
Ruijie (config)# show access-lists
expert access-list extended 2702
10 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

**Related  
Commands**

| Command           | Description                                  |
|-------------------|----------------------------------------------|
| show access-lists | Show all the ACLs.                           |
| mac access-group  | Apply the extended MAC ACL on the interface. |

**Platform  
Description** N/A

## 1.3 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**access-list** *id* **list-remark** *text*

**no access-list** *id* **list-remark**

| Parameter Description | Parameter   | Description                                                                                                                                                                         |
|-----------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>id</i>   | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199. 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
|                       | <i>text</i> | Comment that describes the access list.                                                                                                                                             |

**Defaults** The access lists have no remarks by default.

**Command Mode** Global configuration mode

**Usage Guide** You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

**Configuration Examples** The following example writes a comment of "this acl is to filter the host 192.168.4.12" for ACL100.

```
Ruijie(config)# ip access-list extended 100
Ruijie(config)# access-list 100 list-remark this acl is to filter the host
192.168.4.12
```

| Related Commands | Command                       | Description                                                                                |
|------------------|-------------------------------|--------------------------------------------------------------------------------------------|
|                  | show access- lists            | Displays all access lists, including the remarks for the access lists.                     |
|                  | show access-lists <i>id</i>   | Displays the access list of a specified number, including the remarks for the access list. |
|                  | show access-lists <i>name</i> | Displays the access list of a specified name, including the remarks for the access list.   |

**Platform Description**

## 1.4 access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use the **no** form of this command to remove the remark.

**access-list** *id* **remark** *text*

**no access-list** *id* **remark** *text*

| Parameter Description | Parameter   | Description                                                                                                                                                                         |
|-----------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>id</i>   | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199, 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
|                       | <i>text</i> | Comment that describes the access list entry.                                                                                                                                       |

**Defaults** The access list entries have no remarks by default.

**Command Mode** Global configuration mode

**Usage Guide** You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

**Configuration** The following example writes a comment for an entry in ACL102.

**Examples**

```
Ruijie(config)# access-list 102 remark deny-host-10.1.1.1
```

| Related Commands | Command                       | Description                                                                                      |
|------------------|-------------------------------|--------------------------------------------------------------------------------------------------|
|                  | show access-lists             | Displays all access lists, including the remarks for the access list entries.                    |
|                  | show access-lists <i>id</i>   | Displays the access list of a specified number, including the remarks for the access list entry. |
|                  | show access-lists <i>name</i> | Displays the access list of a specified name, including the remarks for the access list entry.   |

**Platform Description**

## 1.5 action { forward | drop | redirect }

Use this command to set the action for a VLAN access map entry. Use the **no** form of this command to remove the action for the VLAN access map..

**action** { **forward** | **drop** | **redirect** *interface-name* }

**no action** { **forward** | **drop** | **redirect** *interface-name* }

| Parameter   | Parameter             | Description        |
|-------------|-----------------------|--------------------|
| Description | <i>interface-name</i> | Redirect interface |

**Defaults** The VLAN access map entry has no action by default.

**Command Mode** VLAN access-map configuration mode

**Usage Guide** To make the VACL take effect, the action for the VLAN access map entry must be configured. Use the **show vlan access-map** command to display the VLAN access maps created on the device.

**Configuration Examples** The following example sets the action for the VLAN access map `vlan1-map` to **forward**.

```
Ruijie(config)# vlan access-map vlan1-map
Ruijie(config-access-map)# action forward
```

| Related Commands | Command                         | Description                                          |
|------------------|---------------------------------|------------------------------------------------------|
|                  | show access-map                 | Displays all VLAN access maps created on the device. |
|                  | show access-map <i>map-name</i> | Displays the specified VLAN access map..             |

**Platform Description** N/A

## 1.6 clear counters access-list

Use this command to clear counters of packets matching ACLs.

**clear counters access-list** [ *id* | *name* ]

| Parameter   | Parameter   | Description        |
|-------------|-------------|--------------------|
| Description | <i>id</i>   | Access list number |
|             | <i>name</i> | Access list name   |

**Defaults**

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** This command is used to clear the counters of packets matching the specified or all ACLs.

**Configuration** The following example clears the packet matching counter of ACL No. 2700:

**Examples**

```
Ruijie #show access-lists 2700
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (88 matches)
 20 deny tcp any any eq login any any (33455 matches)
 30 permit tcp any any host 192.168.6.9 any (10 matches)

Ruijie# clear counters access-list 2700
Ruijie #show access-lists 2700
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
 20 deny tcp any any eq login any any
 30 permit tcp any any host 192.168.6.9 any
```

**Related Commands**

| Command            | Description                  |
|--------------------|------------------------------|
| expert access-list | Defines an expert ACL.       |
| deny               | Defines a deny ACL entry.    |
| permit             | Defines a permits ACL entry. |

**Platform** N/A  
**Description**

## 1.7 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

- Standard IP ACL

```
[sn] deny {source source-wildcard | host source | any} interface idx][time-range tm-range-name]
[log]
```

- Extended IP ACL

```
[sn] deny protocol source source-wildcard destination destination-wildcard [precedence
precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [log]
```

Extended IP ACLs of some important protocols:

- Internet Control Message Prot (ICMP)



[sn] **deny icmp** {source source-wildcard | **host** source | **any**} {**destination** destination-wildcard | **host** destination | **any**} [icmp-type] [[icmp-type icmp-code] | [icmp-message]] [**precedence** precedence] [**tos** tos] [**fragment**] [**time-range** time-range-name]

- Transmission Control Protocol (TCP)

[sn] **deny udp** {source source-wildcard | **host** source | **any**} [operator **port** [port]] {destination destination-wildcard | **host** destination | **any**} [operator **port** [port]] [**precedence** precedence] [**tos** tos] [**fragment**] [**range** lower upper] [**time-range** time-range-name]

- User Datagram Protocol (UDP)

[sn] **deny udp** {source source-wildcard | **host** source | **any**} [operator **port** [port]] {destination destination-wildcard | **host** destination | **any**} [operator **port** [port]] [**precedence** precedence] [**tos** tos] [**fragment**] [**range** lower upper] [**time-range** time-range-name]

### 3. Extended MAC ACL

[ sn ] **deny** { **any** | **host** source-mac-address } { **any** | **host** destination-mac-address } [ ethernet-type ] [ **cos** [ out ] [ **inner** in ] ]

### 4. Extended expert ACL

[sn] **deny**[**protocol** | [ethernet-type][ **cos** [out] [inner in]]] [[**VID** [out][inner in]]] {source source-wildcard | **host** source | **any**} {**host** source-mac-address | **any**} {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**} [**precedence** precedence] [**tos** tos][**fragment**] [**range** lower upper] [**time-range** time-range-name]

- When you select the ethernet-type field or cos field:

[sn] **deny** {[ethernet-type][**cos** [out] [inner in]]] [[**VID** [out][inner in]]] {source source-wildcard | **host** source | **any**} {**host** source-mac-address | **any**} {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**} [**time-range** time-range-name]

- When you select the protocol field:

[sn] **deny protocol** [[**VID** [out][inner in]]] {source source-wildcard | **host** source | **any**} {**host** source-mac-address | **any**} {destination destination-wildcard | **host** destination | **any**} { **host** destination-mac-address | **any**} [**precedence** precedence] [**tos** tos] [**fragment**] [**range** lower upper] [**time-range** time-range-name]

- Extended expert ACLs of some important protocols

#### Internet Control Message Protocol (ICMP)

[sn] **deny icmp** [[**VID** [out][inner in]]] {source source-wildcard | **host** source | **any**} {**host** source-mac-address | **any**} {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**} [icmp-type] [[icmp-type icmp-code] | [icmp-message]] [**precedence** precedence] [**tos** tos] [**fragment**] [**time-range** time-range-name]

#### Transmission Control Protocol (TCP)

[sn] **deny tcp** [[**VID** [out][inner in]]]{source source-wildcard | **host** Source | **any**} {**host** source-mac-address | **any**} [operator **port** [port]] {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**} [operator **port** [port]] [**precedence** precedence] [**tos** tos] [**fragment**] [**range** lower upper] [**time-range** time-range-name] [**match-all** tcp-flag | **established**]

#### User Datagram Protocol (UDP)

[sn] **deny udp** [[**VID** [out][inner in]]]{source source-wildcard | **host** source | **any**} {**host** source-mac-address | **any**} [operator **port** [port]] {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**} [operator **port** [port]] [**precedence** precedence] [**tos** tos] [**fragment**] [**range** lower upper] [**time-range** time-range-name]

**Address Resolution Protocol (ARP)**

[*sn*] **deny arp** {*vid vlan-id*}[ **host** *source-mac-address* | **any**] [**host** *destination-mac-address* | **any**] {*sender-ip sender-ip-wildcard* | **host** *sender-ip* | **any**} {*sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any**} {*target-ip target-ip-wildcard* | **host** *target-ip* | **any**}

**5. Extended IPv6 ACL**

[*sn*] **deny protocol**{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* } {*destination-ipv6-prefix / prefix-length* | **any**| *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended ipv6 ACLs of some important protocols:

**Internet Control Message Protocol (ICMP)**

[*sn*]**deny icmp** {*source-ipv6-prefix / prefix-length* | *any source-ipv6-address* | **host**} {*destination-ipv6-prefix / prefix-length* | **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

**Transmission Control Protocol (TCP)**

[*sn*] **deny tcp** {*source-ipv6-prefix / prefix-length* | **host***source-ipv6-address* | **any**}[*operator port*[*port*]] {*destination-ipv6-prefix / prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator port* [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

**User Datagram Protocol (UDP)**

[*sn*] **deny udp** {*source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any**} [*operator port* [*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**}[*operator port* [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

**Parameter Description**

| Parameter                       | Description                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------|
| <i>sn</i>                       | ACL entry sequence number                                                               |
| <i>source-ipv6-prefix</i>       | Source IPv6 network address or network type                                             |
| <i>destination-ipv6-prefix</i>  | Destination IPv6 network address or network type                                        |
| <i>prefix-length</i>            | Prefix mask length                                                                      |
| <i>source-ipv6-address</i>      | Source IPv6 address                                                                     |
| <i>destination-ipv6-address</i> | Destination IPv6 address                                                                |
| <i>dscp</i>                     | Differential Service Code Point                                                         |
| <i>dscp</i>                     | Code value, within the range of 0 to 63                                                 |
| <i>flow-label</i>               | Flow label                                                                              |
| <i>flow-label</i>               | Flow label value, within the range of 0 to 1048575.                                     |
| <i>protocol</i>                 | For the IPv6, the field can be ipv6   icmp   tcp   udp and number in the range 0 to 255 |
| <i>time-range</i>               | Time range of the packet filtering                                                      |
| <i>time-range-name</i>          | Time range name of the packet filtering                                                 |

**Defaults**

No entry

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to configure the filtering entry of ACLs in ACL configuration mode.

**Configuration Examples** The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Ruijie(config)#expert access-list extended 2702
Ruijie(config-exp-nacl)#deny tcp host
192.168.4.12 host 0013.0049.8272 any any
Ruijie(config-exp-nacl)#permit any any any any
Ruijie(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp host 192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
Ruijie(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)# ip access-list extended ip-ext-acl
Ruijie(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ip access-group ip-ext-acl in
Ruijie(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#mac access-list extended mac1
Ruijie(config-mac-nacl)#deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ip access-list standard 34
```

```
Ruijie(config-ext-nacl)# deny host 192.168.4.12
Ruijie(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
Ruijie(config-ext-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ip access-group 34 in
```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#11 deny ipv6 host 192.168.4.12 any
Ruijie(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ipv6 traffic-filter v6-acl in
```

#### Related Commands

| Command             | Description                                     |
|---------------------|-------------------------------------------------|
| show access-lists   | Displays all ACLs.                              |
| ipv6 traffic-filter | Applies the extended IPv6 ACL on the interface. |
| ip access-group     | Applies the IP ACL on the interface.            |
| mac access-group    | Applies the extended MAC ACL on the interface.  |
| ip access-list      | Defines an IP ACL.                              |
| mac access-list     | Defines an extended MAC ACL.                    |
| expert access-list  | Defines an extended expert ACL.                 |
| ipv6 access-list    | Defines an extended IPv6 ACL.                   |
| permit              | Permits the access.                             |

**Platform** N/A

**Description**

## 1.8 expert access-group

Use this command to apply the specified expert access list globally or on the specified interface. Use the **no** form of the command to remove the application.

**expert access-group** { *id* | *name* } { **in** | **out** }

**no expert access-group** { *id* | *name* } { **in** | **out** }

| Parameter Description | Parameter   | Description                              |
|-----------------------|-------------|------------------------------------------|
|                       | <i>id</i>   | Expert access list number: 2700 to 2899  |
|                       | <i>name</i> | Name of the expert access list           |
|                       | in          | Specifies filtering on inbound packets.  |
|                       | out         | Specifies filtering on outbound packets. |

**Defaults** No expert access list is applied globally or on the interface.

**Command mode** Global, interface configuration mode.

**Usage Guide** This command is used to apply the specified access list globally or on the interface to control the input and output data streams. Use the **show access-group** command to view the setting.

**Configuration Examples** The following example shows how to apply the **access-list accept\_00d0f8xxxxxx** only to Gigabit interface 0/1:

```
Ruijie(config)# interface GigaEthernet 0/1
Ruijie(config-if)# expert access-group
accept_00d0f8xxxxxx_only in
```

| Related Commands | Command           | Description                     |
|------------------|-------------------|---------------------------------|
|                  | show access-group | Displays the ACL configuration. |

**Platform Description** N/A

## 1.9 expert access-list advanced

Use this command to create an advanced expert access list and place the device in expert advanced access list configuration mode. Use the **no** form of this command to remove the advanced expert access list.

**expert access-list advanced** *name*

**no expert access-list advanced** *name*

| Parameter Description | Parameter   | Description                             |
|-----------------------|-------------|-----------------------------------------|
|                       | <i>name</i> | Name of the advanced expert access list |

**Defaults** N/A

**Command** Global configuration mode

**mode**

**Usage Guide** Use this command to create an advanced expert access list (namely, ACL80) to match your custom fields.

**Configuration** The following example creates an advanced expert access list named adv-acl.

**Examples**

```
Ruijie(config)# expert access-list advanced adv-acl
Ruijie(config-exp-dacl)# show access-lists
expert access-list advanced adv-acl
```

**Related Commands**

| Command                       | Description                                   |
|-------------------------------|-----------------------------------------------|
| show access-lists             | Displays all access lists.                    |
| show access-lists <i>name</i> | Displays the access list of a specified name. |

**Platform** N/A

**Description**

## 1.10 counter

Use this command to enable the counter of packets matching the specified expert access list. Use the **no** form of this command to disable this function.

**expert access-list counter** { *id* | *name* }

**no expert access-list counter** { *id* | *name* }

**Parameter Description**

| Parameter   | Description                              |
|-------------|------------------------------------------|
| <i>id</i>   | Expert access list number: 2700 to 2899. |
| <i>name</i> | Name of the access list.                 |

**Defaults** The counter of the packets matching the expert access list is disabled.

**Command mode** Global configuration mode

**Usage Guide** Use this command to enable the counter of packets matching the specified expert access list, so that you can analyze the counters to learn whether the network is attacked by the illegal packets.

**Configuration Examples** The following example enables the counter of packets matching the extended expert access list named exp-acl:

```
Ruijie(config)# expert access-list counter exp-acl
Ruijie(config)# show access-lists
expert access-list extended exp-acl
```

```
10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (16 matches)
20 deny tcp any any eq login any any (78 matches)
```

The following example disables the counter of packets matching the extended expert access list named exp-acl.

```
Ruijie(config)#no expert access-list counter exp-acl
Ruijie(config)# show access-lists
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
 20 deny tcp any any eq login any any
```

#### Related Commands

| Command           | Description                       |
|-------------------|-----------------------------------|
| show access-lists | Displays the extended expert ACL. |

#### Platform

N/A

#### Description

## 1.11 expert access-list extended

Use this command to create an extended expert access list. Use the **no** form of the command to remove the ACL.

**expert access-list extended** {*id* | *name*}

**no expert access-list extended** {*id* | *name*}

#### Parameter Description

| Parameter   | Description                                      |
|-------------|--------------------------------------------------|
| <i>id</i>   | Extended expert access list number: 2700 to 2899 |
| <i>name</i> | Name of the extended expert access list          |

#### Defaults

N/A

#### Command mode

Global configuration mode.

#### Usage Guide

Use the **show access-lists** command to display the ACL configurations.

#### Configuration Examples

Create an extended expert ACL named exp-acl:

```
Ruijie(config)# expert access-list extended exp-acl
Ruijie(config-exp-nacl)# show access-lists expert access-list extended
exp-acl
Ruijie(config-exp-nacl)#
```

Create an extended expert ACL numbered 2704:

```
Ruijie(config)# expert access-list extended 2704
```

```
Ruijie(config-exp-nacl)# show access-lists access-list extended 2704
Ruijie(config-exp-nacl)#
```

**Related  
Commands**

| Command                  | Description                       |
|--------------------------|-----------------------------------|
| <b>show access-lists</b> | Displays the extended expert ACLs |

**Platform** N/A  
**Description**

## 1.12 expert access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

**expert access-list new-fragment-mode** { *id* | *name* }

**no expert access-list new-fragment-mode** { *id* | *name* }

**Parameter  
Description**

| Parameter   | Description                              |
|-------------|------------------------------------------|
| <i>id</i>   | Expert access list number: 2700 to 2899. |
| <i>name</i> | Name of the expert access list.          |

**Defaults** Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

**Command mode** Global configuration mode

**Usage Guide** Use this command to switch and control the matching mode of access rules to fragmentation packets.

**Configuration Examples** The following example switches the matching mode of fragmentation packets for the ACL 2700 from the default mode to a new matching mode:

```
Ruijie(config)#expert access-list new-fragment-mode 2700
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| -       | -           |

**Platform** N/A  
**Description**



## 1.13 expert access-list resequence

Use this command to resequence an expert access list. Use the no form of this command to restore the default order of access entries.

**expert access-list resequence** { *id* | *name* } *start-sn* *inc-sn*

**no expert access-list resequence** { *id* | *name* }

| Parameter Description | Parameter       | Description                                              |
|-----------------------|-----------------|----------------------------------------------------------|
|                       | <i>id</i>       | Expert access list number: 2700 to 2899.                 |
|                       | <i>name</i>     | Name of the expert access list                           |
|                       | <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647            |
|                       | <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults**      *start-sn*: 10  
                   *inc-sn*: 10

**Command mode**      Global configuration mode

**Usage Guide**      Use this command to change the order of the access entries.

**Configuration Examples**      The following example resequences entries of expert access list "exp-acl":

**Examples**      Before the configuration:

```
Ruijie# show access-lists
expert access-list extended exp-acl
 10 permit ip any any any any
 20 deny ip any any any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# expert access-list resequence exp-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
expert access-list extended exp-acl
 21 permit ip any any any any
 64 deny ip any any any any
```

| Related Commands | Command           | Description                 |
|------------------|-------------------|-----------------------------|
|                  | show access-lists | Displays all access lists.. |

**Platform Description**      N/A

## 1.14 global ip access-group

Use this command to apply the global IP-based access list on the interface. Use the **no** form of this command to remove the global IP-based access list from the interface.

**global ip access-group**

**no global ip access-group**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** By default, the global IP-based access list is applied on the interface.

**Command mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example applies the global IP-based access list on interface fastEthernet0/0.

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#global ip access-group
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.15 ip access-group

Use this command to apply a specific access list globally or to an interface or VXLAN. Use the **no** form of this command to remove the access list from the interface.

**ip access-group** {*id* | *name*} {**in** | **out**} [**reflect**] [**control-plane**]

**no ip access-group** { *id* | *name*} {**in** | **out**} [**control-plane**]

| Parameter Description | Parameter   | Description                                                                 |
|-----------------------|-------------|-----------------------------------------------------------------------------|
|                       | <i>id</i>   | IP access list or extended IP access list number:<br>1 to 199, 1300 to 2699 |
|                       | <i>name</i> | Name of the IP ACL                                                          |
|                       | <b>in</b>   | Filters the incoming packets of the interface.                              |

|     |                                                |
|-----|------------------------------------------------|
| out | Filters the outgoing packets of the interface. |
|-----|------------------------------------------------|

**Defaults** No access list is applied globally or on the interface by default.

**Command mode** Global, interface configuration mode.

**Usage Guide** Use this command to control access to a specified interface, globally.

**Configuration Examples** The following example applies the ACL 120 on interface fastEthernet0/0 to filter the incoming packets:

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if)# ip access-group 120 in
```

**Related Commands**

| Command           | Description        |
|-------------------|--------------------|
| access-list       | Defines an ACL.    |
| show access-lists | Displays all ACLs. |

**Platform** N/A

**Description**

## 1.16 ip access-list

Use this command to create a standard IP access list or extended IP access list. Use the **no** form of the command to remove the access list.

**ip access-list** {**extended** | **standard**} {*id* | *name*}

**no ip access-list** {**extended** | **standard**} {*id* | *name*}

**Parameter Description**

| Parameter   | Description                                                                                    |
|-------------|------------------------------------------------------------------------------------------------|
| <i>id</i>   | Access list number:<br>Standard: 1 to 99, 1300 to 1999;<br>Extended: 100 to 199, 2000 to 2699. |
| <i>name</i> | Name of the access list                                                                        |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list. Refer to **deny** or **permit** in the two modes. Use the **show access-lists** command to display the ACL

configurations.

**Configuration** The following example creates a standard access list named std-acl.

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
Ruijie(config-std-nacl)#
```

The following example creates an extended ACL numbered 123:

```
Ruijie(config)# ip access-list extended 123
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 123
```

**Related  
Commands**

| Command           | Description        |
|-------------------|--------------------|
| show access-lists | Displays all ACLs. |

**Platform** N/A  
**Description**

## 1.17 ip access-list counter

Use this command to enable the counter of packets matching the standard or extended IP access list. Use the **no** form of this command to disable the counter.

```
ip access-list counter { id | name }
no ip access-list counter { id | name }
```

**Parameter  
Description**

| Parameter   | Description                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| <i>id</i>   | IP access list number:<br>Standard IP access list: 1 to 99, 1300 to 1999;<br>Extended IP access list: 100 to 199, 2000 to 2699. |
| <i>name</i> | Name of the IP access list.                                                                                                     |

**Defaults** The counter of packets matching the standard or extended IP access list is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enables the counter of packets matching the standard access list:

```
Ruijie(config)# ip access-list counter std-acl
```

```
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255 (999 matches)
 20 deny host 5.5.5.5 time-range tm (2000 matches)
```

The following example disables the counter of packets matching the standard access list:

```
Ruijie(config)#no ip access-list counter std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255
 20 deny host 5.5.5.5 time-range tm
```

#### Related Commands

| Command           | Description                |
|-------------------|----------------------------|
| show access-lists | Displays all access lists. |

#### Platform

N/A

#### Description

## 1.18 ip access-list log-update interval

Use this command to configure the interval at which the IPv4 access list log is updated. Use the **no** form of this command to restore the default interval.

**ip access-list log-update interval** *time*

**no ip access-list log-update interval**

#### Parameter Description

| Parameter   | Description                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>time</i> | For the access rule with the <b>log</b> option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specified flow is output every 5 minutes. 0 indicates that no ACL logging is output. |

#### Defaults

The default interval at which the IPv4 access list log is updated is 5 minutes.

#### Command mode

Global configuration mode

#### Usage Guide

Use this command to configure the interval at which the IPv4 access list log is updated.

**Configuration** The following example configures the interval for the IPv4 access list log update to 10 minutes:

**Examples**

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ip access-list log-update interval 10
```

**Related Commands**

| Command        | Description                                    |
|----------------|------------------------------------------------|
| ip access-list | Defines an IPv4 access list.                   |
| deny           | Defines the <b>deny</b> access entries.        |
| permit         | Defines the <b>permit</b> access entries.      |
| show running   | Displays running configurations of the device. |

**Platform**

N/A

**Description**

## 1.19 ip access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets of standard or extended IP access list. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

**ip access-list new-fragment-mode** { *id* | *name* }

**no ip access-list new-fragment-mode** { *id* | *name* }

**Parameter Description**

| Parameter   | Description                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| <i>id</i>   | IP access list number:<br>Standard IP access list: 1 to 99, 1300 to 1999;<br>Extended IP access list: 100 to 199, 2000 to 2699. |
| <i>name</i> | Name of the standard or extended IP access list                                                                                 |

**Defaults**

Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

**Command mode**

Global configuration mode

**Usage Guide**

This command is used to switch and control the fragmentation packet matching mode of access rules.

**Configuration Examples**

The following example switches the fragmentation packet matching mode of the ACL 100 from the default mode to a new mode:

```
Ruijie(config)#ip access-list new-fragment-mode 100
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.20 ip access-list resequence

Use this command to resequence a standard or extended IP access list. Use the **no** form of this command to restore the default order of access entries.

**ip access-list resequence** { *id* | *name* } *start-sn* *inc-sn*

**no ip access-list resequence** { *id* | *name* }

| Parameter Description | Parameter       | Description                                                                                                                     |
|-----------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>id</i>       | IP access list number:<br>Standard IP access list: 1 to 99, 1300 to 1999;<br>Extended IP access list: 100 to 199, 2000 to 2699. |
|                       | <i>name</i>     | Name of the standard or extended IP access list                                                                                 |
|                       | <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647                                                                                   |
|                       | <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647                                                                        |

**Defaults** *start-sn*: 10  
*inc-sn*: 10

**Command mode** Global configuration mode

**Usage Guide** Use this command to change the order of the access entries.

**Configuration** The following example resequences entries of ACL1:

**Examples** Before the configuration:

```
Ruijie# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# ip access-list resequence 1 21 43
Ruijie(config)# exit
Ruijie# show access-lists
```

```
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

**Related  
Commands**

| Command           | Description                 |
|-------------------|-----------------------------|
| show access-lists | Displays all access lists.. |

**Platform** N/A  
**Description**

## 1.21 ipv6 access-list

Use this command to create an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.

**ipv6 access-list** *name*  
**no ipv6 access-list** *name*

**Parameter  
Description**

| Parameter   | Description                   |
|-------------|-------------------------------|
| <i>name</i> | Name of the IPv6 access list. |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** To filter the IPv6 packets through the access list, you need to define an IPv6 access list by using the **ipv6 access-list** command.

**Configuration Examples** The following example creates an IPv6 access list named v6-acl:

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#
```

**Related  
Commands**

| Command           | Description                |
|-------------------|----------------------------|
| show access-lists | Displays all access lists. |

**Platform** N/A  
**Description**



## 1.22 ipv6 access-list counter

Use this command to enable the counter of packets matching the IPv6 access list. Use the **no** form of this command to disable the counter.

**ipv6 access-list counter** *name*

**no ipv6 access-list counter** *name*

| Parameter Description | Parameter   | Description                   |
|-----------------------|-------------|-------------------------------|
|                       | <i>name</i> | Name of the IPv6 access list. |

**Defaults** -

**Command mode** Global configuration mode

**Usage Guide** Use this command to enable the counter of packets matching the IPv6 access list to monitor the IPv6 packets matching and filtering.

**Configuration Examples** The following example enables the counter of packets matching the IPv6 access list named v6-acl:

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any (7 matches)
 20 deny tcp any any (7 matches)
```

The following example disables the counter of packets matching the IPv6 access list named v6-acl:

```
Ruijie(config)#no ipv6 access-list v6-acl counter
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any
 20 deny tcp any any
```

| Related Commands | Command           | Description                |
|------------------|-------------------|----------------------------|
|                  | show access-lists | Displays all access lists. |

**Platform Description** N/A

## 1.23 ipv6 access-list log-update interval

Use this command to configure the interval at which the IPv6 access list log is updated. Use the **no**

form of this command to restore the default interval.

**ipv6 access-list log-update interval** *time*

**no ipv6 access-list log-update interval**

| Parameter Description | Parameter   | Description                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>time</i> | For the access rule with the <b>logging</b> option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specific flow is output every 5 minutes. 0 indicates that no ACL logging is output. |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Use this command to configure the interval at which the IPv6 access list log is updated.

**Configuration Examples** The following example configures the interval for the IPv6 access list log update to 10 minutes:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# ipv6 access-list log-update interval 9
```

| Related Commands | Command          | Description                                        |
|------------------|------------------|----------------------------------------------------|
|                  | ipv6 access-list | Defines an IPv6 access list.                       |
|                  | deny             | Defines the <b>deny</b> access entries.            |
|                  | permit           | Defines the <b>permit</b> access entries.          |
|                  | show running     | Displays the running configurations of the device. |

**Platform Description** N/A

## 1.24 ipv6 access-list resequence

Use this command to resequence an IPv6 access list. Use the **no** form of this command to restore the default order of access entries.

**ipv6 access-list resequence** *name start-sn inc-sn*

**no ipv6 access-list resequence** *name*

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|                 |                                                          |
|-----------------|----------------------------------------------------------|
| <i>name</i>     | Name of the IPv6 access list                             |
| <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647            |
| <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults**      *start-sn*: 10  
*inc-sn*: 10

**Command mode**      Global configuration mode

**Usage Guide**      Use this command to change the order of the access entries.

**Configuration**      The following example resequences entries of IPv6 access list "v6-acl":

**Examples**      Before the configuration:

```
Ruijie# show access-lists
ipv6 access-list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# ipv6 access-list resequence v6-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
ipv6 access-list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any
```

**Related Commands**

| Command           | Description                 |
|-------------------|-----------------------------|
| show access-lists | Displays all access lists.. |

**Platform**      N/A

**Description**

## 1.25 ipv6 traffic-filter

Use this command to apply an IPV6 access list on the specified interface. Use the **no** form of the command to remove the IPV6 access list from the interface/VXLAN.

**ipv6 traffic-filter** *name* { **in** | **out** }

**no ipv6 traffic-filter** *name* { **in** | **out** }

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|             |                                         |
|-------------|-----------------------------------------|
| <i>name</i> | Name of IPv6 access list                |
| in          | Specifies filtering on inbound packets  |
| out         | Specifies filtering on outbound packets |

**Defaults** N/A

**Command mode** Interface configuration mode.

**Usage Guide** Use this command to apply the IPv6 access list to a specified interface to filter the inbound or outbound packets.

**Configuration Examples** The following example applies the IPv6 access list named **v6-acl** to interface GigabitEthernet 0/1:

```
Ruijie(config)# interface GigaEthernet 0/1
Ruijie(config-if)# ipv6 traffic-filter v6-acl in
```

**Related Commands**

| Command           | Description                                   |
|-------------------|-----------------------------------------------|
| show access-group | Displays ACL configurations on the interface. |

**Platform** N/A

**Description**

## 1.26 list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**list-remark** *text*

**no list-remark**

**Parameter Description**

| Parameter   | Description                             |
|-------------|-----------------------------------------|
| <i>text</i> | Comment that describes the access list. |

**Defaults** The access lists have no remarks by default.

**Command mode** ACL configuration mode

**Usage Guide** You can use this command to write a helpful comment for a specified access list.

**Configuration Examples** The following example writes a comment of "this acl is to filter the host 192.168.4.12" for ACL102.

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# list-remark this acl is to filter the host
```

```

192.168.4.12
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
Ruijie(config-ext-nacl)#

```

#### Related Commands

| Command                 | Description                                                             |
|-------------------------|-------------------------------------------------------------------------|
| show access-lists       | Displays all access lists.                                              |
| ip access-list          | Defines an IPv4 access list.                                            |
| access-list list remark | Adds a helpful comment for an access list in global configuration mode. |

**Platform** N/A

#### Description

## 1.27 mac access-group

Use this command to apply the specified MAC access list globally or on the specified interface . Use the **no** form of the command to remove the access list from the interface.

**mac access-group** { *id* | *name* } { **in** | **out** }

**no mac access-group** { *id* | *name* } { **in** | **out** }

#### Parameter Description

| Parameter   | Description                                           |
|-------------|-------------------------------------------------------|
| <i>id</i>   | MAC access list number. The range is from 700 to 799. |
| <i>name</i> | Name of the MAC access list                           |
| in          | Specifies filtering on the inbound packets.           |
| out         | Specifies filtering on the outbound packets.          |

**Defaults** No MAC access list is applied by default.

**Command mode** Global, interface configuration mode.

**Usage Guide** Use this command to apply the access list globally or to the interface or VXLAN to filter the inbound or outbound packets based on the MAC address.

**Configuration Examples** The following example applies the MAC access-list **accept\_00d0f8xxxxxx\_only** to interface GigabitEthernet 1/1:

```
Ruijie(config)# interface GigaEthernet 1/1
```

```
Ruijie(config-if-GigabitEthernet 1/1)# mac access-group
accept_00d0f8xxxxxx_only in
```

**Related  
Commands**

| Command           | Description                                      |
|-------------------|--------------------------------------------------|
| show access-group | Displays the ACL configuration on the interface. |

**Platform** N/A  
**Description**

## 1.28 mac access-list counter

Use this command to enable the counter of packet matching the extended MAC access list. Use the **no** form of this command to disable the counter.

**mac access-list counter** { *id* | *name* }

**no mac access-list counter** { *id* | *name* }

**Parameter  
Description**

| Parameter   | Description                                                    |
|-------------|----------------------------------------------------------------|
| <i>id</i>   | Extended MAC access list number. The range is from 700 to 799. |
| <i>name</i> | Name of the extended MAC access list                           |

**Defaults** The counter is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** Use this command to enable the counter of packets matching the MAC access list to monitor the packets matching and filtering.

**Configuration Examples** The following example enables the counter of packet matching the extended MAC access list named mac-acl:

```
Ruijie(config)# mac access-list counter mac-acl
Ruijie(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any (170 matches)
 20 deny any any etype-any cos 6 (239 matches)
```

The following example disables the counter of packet matching the extended MAC access list named mac-acl:

```
Ruijie(config)#no mac access-list counter mac-acl
Ruijie(config)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any
 20 deny any any etype-any cos 6
```

| Related Commands | Command           | Description                |
|------------------|-------------------|----------------------------|
|                  | show access-lists | Displays all access lists. |

**Platform** N/A  
**Description**

## 1.29 mac access-list extended

Use this command to create an extended MAC access list. Use the **no** form of the command to remove the MAC access list.

**mac access-list extended** { *id* | *name* }

**no mac access-list extended** { *id* | *name* }

| Parameter Description | Parameter                            | Description                                                    |
|-----------------------|--------------------------------------|----------------------------------------------------------------|
|                       | <i>id</i>                            | Extended MAC access list number. The range is from 700 to 799. |
| <i>name</i>           | Name of the extended MAC access list |                                                                |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** To filter the packets based on the MAC address, you need to define a MAC access list by using the **mac access-list extended** command.

**Configuration** The following command creates an extended MAC access list named mac-acl:

**Examples**

```
Ruijie(config)# mac access-list extended mac-acl
```

```
Ruijie(config-mac-nacl)# show access-lists mac access-list extended mac-acl
```

The following command creates an extended MAC access list numbered 704:

```
Ruijie(config)# mac access-list extended 704
```

```
Ruijie(config-mac-nacl)# show access-lists mac access-list extended 704
```

| Related Commands | Command           | Description                |
|------------------|-------------------|----------------------------|
|                  | show access-lists | Displays all access lists. |

**Platform** N/A  
**Description**

## 1.30 mac access-list resequence

Use this command to resequence an extended MAC access list. Use the **no** form of this command to restore the default order of access entries.

**mac access-list resequence** { *id* | *name* } *start-sn inc-sn*

**no mac access-list resequence** { *id* | *name* }

| Parameter Description | Parameter       | Description                                              |
|-----------------------|-----------------|----------------------------------------------------------|
|                       | <i>id</i>       | Extended MAC access list number: 700 to 799.             |
|                       | <i>name</i>     | Name of the extended MAC access list                     |
|                       | <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647            |
|                       | <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults**      *start-sn*: 10  
                   *inc-sn*: 10

**Command mode**      Global configuration mode

**Usage Guide**      Use this command to change the order of the access entries.

**Configuration Examples**      The following example resequences entries of extended MAC access list "mac-acl":

**Examples**      Before the configuration:

```
Ruijie# show access-lists
mac access-list extended mac-acl
 10 permit any any etype-any
 20 deny any any etype-any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# mac access-list resequence exp-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
mac access-list extended mac-acl
 21 permit any any etype-any
 64 deny any any etype-any
```

| Related Commands | Command           | Description                 |
|------------------|-------------------|-----------------------------|
|                  | show access-lists | Displays all access lists.. |

**Platform Description**      N/A



## 1.31 permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

### 1. Standard IP ACL

```
[sn] permit {source source-wildcard | host source | any | interface idx } [time-range tm-range-name] [log]
```

### 2. Extended IP ACL

```
[sn] permit protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [log]
```

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[sn] permit icmp {source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]] [precedence precedence] [tos tos] [fragment] [time-range time-range-name]
```

Transmission Control Protocol (TCP)

```
[sn] permit tcp { source source-wildcard | host source | any } [operator port [port]] { destination destination-wildcard | host destination | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag | established]
```

User Datagram Protocol (UDP)

```
[sn] permit udp {source source-wildcard|host source|any} [operator port [port]] {destination destination-wildcard|host destination|any} [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]
```

### 3. Extended MAC ACL

```
[sn] permit { any | host source-mac-address | source-mac-address mask } { any | host destination-mac-address | destination-mac-address mask } [ethernet-type] [cos [out] [inner in]]
```

### 4. Extended expert ACL

```
[sn] permit [protocol | [ethernet-type] [cos [out] [inner in]]] [VID [out][inner in]] {source source-wildcard | host source | any} {host source-mac-address | any} {destination destination-wildcard | host destination | any} {host destination-mac-address | any} [precedence precedence] [tos tos][fragment] [range lower upper] [time-range time-range-name]
```

When you select the Ethernet-type field or cos field:

```
[sn] permit {ethernet-type| cos [out] [inner in]} [VID [out][inner in]] {source source-wildcard | host source | any} {host source-mac-address | any} {destination destination-wildcard | host destination | any} {host destination-mac-address | any} [time-range time-range-name]
```

When you select the protocol field:

```
[sn] permit protocol [VID [out][inner in]] {source source-wildcard | host Source | any} {host source-mac-address | any} {destination destination-wildcard | host destination | any} {host destination-mac-address | any} [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]
```

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[sn] **permit icmp** [VID [out][inner in]] {source source-wildcard | **host** source | **any**} {**host** source-mac-address | **any**} {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**}[ icmp-type ][ [icmp-type [icmp-code ]] | [ icmp-message ]]  
**[precedence precedence]** **[tos tos]** **[fragment]** **[time-range time-range-name]**

Transmission Control Protocol (TCP)

[sn] **permit tcp** [VID [out][inner in]]{source source-wildcard | **host** Source | **any**} {**host** source-mac-address | **any**} [operator **port** [port]] {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**} [operator **port** [port]] **[precedence precedence]** **[tos tos]** **[fragment]** **[range lower upper]** **[time-range time-range-name]** **[match-all tcp-flag | established]**

User Datagram Protocol (UDP)

[sn] **permit udp** [VID [out][inner in]]{source source-wildcard | **host** source | **any**} {**host** source-mac-address | **any**} [ operator **port** [port]] {destination destination-wildcard | **host** destination | **any**} {**host** destination-mac-address | **any**} [operator **port** [port]] **[precedence precedence]** **[tos tos]** **[fragment]** **[range lower upper]** **[time-range time-range-name]**

Address Resolution Protocol (ARP)

[sn] **permit arp** {**vid vlan-id**} [**host** source-mac-address | **any**] [**host** destination-mac-address | **any**] {sender-ip sender-ip-wildcard | **host** sender-ip | **any**} {sender-mac sender-mac-wildcard | **host** sender-mac | **any**} {target-ip target-ip-wildcard | **host** target-ip | **any**}

5. Extended IPv6 ACL

[sn] **permit protocol** {source-ipv6-prefix / prefix-length | **any** | **host** source-ipv6-address} {destination-ipv6-prefix / prefix-length | **any**| hostdestination-ipv6-address} **[dscp dscp]** **[flow-label flow-label]** **[fragment]** **[range lower upper]** **[time-range time-range-name]**

Extended IPv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[sn] **permit icmp** {source-ipv6-prefix / prefix-length | **any** source-ipv6-address | **host**} {destination-ipv6-prefix / prefix-length | **host** destination-ipv6-address | **any**} [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]] **[dscp dscp]** **[flow-label flow-label]****[fragment]** **[time-range time-range-name]**

Transmission Control Protocol (TCP)

[sn] **permit tcp** {source-ipv6-prefix / prefix-length | **host** source-ipv6-address | **any**} [operator **port** [port]] {destination-ipv6-prefix / prefix-length | **host** destination-ipv6-address | **any**} [operator **port** [port]] **[dscp dscp]** **[flow-label flow-label]** **[fragment]** **[range lower upper]** **[time-range time-range-name]** **[match-all tcp-flag | established]**

User Datagram Protocol (UDP)

[sn] **permit udp** {source-ipv6-prefix / prefix-length | **host** source-ipv6-address | **any**} [operator **port** [port]] {destination-ipv6-prefix / prefix-length | **host** destination-ipv6-address | **any**} [operator **port** [port]] **[dscp dscp]** **[flow-label flow-label]** **[fragment]** **[range lower upper]** **[time-range time-range-name]**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

Defaults N/A

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.

**Configuration Examples** The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Ruijie(config)#expert access-list extended exp-acl
Ruijie(config-exp-nacl)#permit tcp host 192.168.4.12 host 0013.0049.8272
any any
Ruijie(config-exp-nacl)#deny any any any any
Ruijie(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp host 192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
Ruijie(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ip access-group 102 in
Ruijie(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#mac access-list extended 702
Ruijie(config-mac-nacl)#permit host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
Ruijie(config-mac-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ip access-list standard std-acl
Ruijie(config-std-nacl)#permit host 192.168.4.12
Ruijie(config-std-nacl)#show access-lists
ip access-list standard std-acl
 10 permit host 192.168.4.12
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
 11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ipv6 traffic-filter v6-acl in
```

#### Related Commands

| Command           | Description                |
|-------------------|----------------------------|
| show access-lists | Displays all access lists. |

#### Platform

N/A

#### Description

## 1.32 redirect destination interface

Use this command to redirect the traffic matching the access list to the specified interface. Use the **no** form of this command to remove the redirection.

**redirect destination interface** *interface-name* **acl** { *id* | *name* } **in**

**no redirect destination interface** *interface-name* **acl** { *id* | *name* } **in**

#### Parameter Description

| Parameter             | Description        |
|-----------------------|--------------------|
| <i>interface-name</i> | Redirect interface |
| <i>id</i>             | Access list number |
| <i>name</i>           | Access list name   |

#### Defaults

No redirection is configured.

#### Command mode

Interface configuration mode

**Usage Guide** Use this command to configure access redirection, namely, to redirect the traffic matching the access list to the specified interface. You can monitor the operation of a specified access list by using this command.

**Configuration** The following example configures access redirection.

**Examples**

```
Ruijie(config)# interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)# redirect destination interface
gigabitEthernet 0/2 acl1 in
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.33 remark

Use this command to write a helpful comment (remark) for an entry in the access list. Use the **no** form of this command to remove the remark.

**remark** *text*

**no** remark

**Parameter  
Description**

| Parameter   | Description                              |
|-------------|------------------------------------------|
| <i>text</i> | Comment that describes the access entry. |

**Defaults** The access entries have no remarks.

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to write a helpful comment for an access entry.  
Up to 100 characters are allowed in the remark.  
Two identical access entry remarks in one access list is not allowed.  
Removing an access entry may delete the remark for it as well.

**Configuration** The following example writes remarks for the entry in extended IP access list 102.

**Examples**

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# remark first_remark
Ruijie(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
Ruijie(config-ext-nacl)# remark second_remark
```

```
Ruijie(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
Ruijie(config-ext-nacl)# end
Ruijie#
```

**Related  
Commands**

| Command           | Description                |
|-------------------|----------------------------|
| show access-lists | Displays all access lists. |

**Platform** N/A  
**Description**

## 1.34 security access-group

Use this command to configure an interface secure channel.

**security access-group** { *id* | *name* }

**no security access-group**

**Parameter  
Description**

| Parameter   | Description              |
|-------------|--------------------------|
| <i>id</i>   | Access list number.      |
| <i>name</i> | Name of the access list. |

**Defaults** N/A

**Command mode** Interface or VXLAN configuration mode

**Usage Guide** If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a secure channel for the users on the specified interface to access the external network without authentication.

**Configuration** The following example configures a secure channel on interface GigaEthernet 1/1:

**Examples**

```
Ruijie(config)# interface GigaEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# security access-group 1
```

**Related  
Commands**

| Command       | Description                                |
|---------------|--------------------------------------------|
| show secu-acl | Displays the secure channel configuration. |

**Platform** N/A  
**Description**

## 1.35 security global access-group

Use this command to configure the global secure channel.

**security global access-group** { *id* | *name* }

**no security global access-group**

| Parameter Description | Parameter   | Description              |
|-----------------------|-------------|--------------------------|
|                       | <i>id</i>   | Access list number.      |
|                       | <i>name</i> | Name of the access list. |

**Defaults** -

**Command mode** Global configuration mode

**Usage Guide** If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a global secure channel for some users to access the external network without authentication.

**Configuration Examples** The following example configures a global secure channel.

```
Ruijie(config)#security global access-group 1
```

| Related Commands | Command       | Description                                 |
|------------------|---------------|---------------------------------------------|
|                  | show secu-acl | Displays the secure channel configuration.. |

**Platform** N/A

**Description**

## 1.36 security uplink enable

Use this command to configure an exceptional interface of the global secure channel.

**security uplink enable**

**no security uplink enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The global secure channel takes effect on all interfaces by default.

**Command mode** Interface configuration mode.

**Usage Guide** The global secure channel takes effect on all interfaces by default. To disable the secure channel function on some interfaces, you can use this command to configure the interface as exceptional.

**Configuration Examples** The following example configures interface GigabitEthernet 1/1 as an exceptional interface of the secure channel.

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# security uplink enable
```

**Related Commands**

| Command       | Description                                |
|---------------|--------------------------------------------|
| show secu-acl | Displays the secure channel configuration. |

**Platform Description** N/A

## 1.37 show access-group

Use this command to display the access list applied to the interface.

**show access-group** [ **interface** *interface-name* ] | [**vxlan vni**]

**Parameter Description**

| Parameter        | Description    |
|------------------|----------------|
| <i>interface</i> | Interface name |

**Defaults** -

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the access list configuration on the specified interface. If no interface is specified, access list configuration on all interfaces is displayed.

**Configuration Examples** Ruijie# show access-group

```
ip access-list standard ipstd3
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4
Applied On interface GigabitEthernet 0/2.
ip access-list extended 101
Applied On interface GigabitEthernet 0/3.
ip access-list extended 102 in
```



**Description****1.38 show access-lists**

Use this command to display all access lists or the specified access list.

**show access-lists** [ *id* | *name* ] [ **summary** ]

| Parameter Description | Parameter   | Description                |
|-----------------------|-------------|----------------------------|
|                       | <i>id</i>   | Access list number         |
|                       | <i>name</i> | Name of the IP access list |
|                       | summary     | Access list summary        |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.

**Configuration Examples**

```
Ruijie# show access-lists n_acl
ip access-list standard n_acl
Ruijie# show access-lists 102
ip access-list extended 102
Ruijie# show access-lists
ip access-list standard n_acl
ip access-list extended 101
permit icmp host 192.168.1.1 any log (1080 matches)
 permit tcp host 1.1.1.1 any established
 deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
petmit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

**1.39 show expert access-group**

Use this command to display the expert access list applied to the interface.

**show expert access-group** [ **interface** *interface-name* ]

| Parameter<br>Description | Parameter | Description      |
|--------------------------|-----------|------------------|
|                          |           | <i>interface</i> |

**Defaults** -

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the expert access list configured on the interface. If no interface is specified, the expert access lists on all interfaces are displayed.

**Configuration Examples**

```
Ruijie# show expert access-group interface gigabitethernet 0/2
expert access-group ee in
Applied On interface GigabitEthernet 0/2.
```

| Related<br>Commands | Command | Description        |
|---------------------|---------|--------------------|
|                     |         | expert access-list |

**Platform Description** N/A

## 1.40 show ip access-group

Use this command to display the standard and extended IP access lists on the interface.

**show ip access-group [ interface *interface* ]**

| Parameter<br>Description | Parameter | Description                            |
|--------------------------|-----------|----------------------------------------|
|                          |           | <b>interface</b> <i>Interface-name</i> |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the standard and extended IP access lists configured on the interface. If no interface is specified, the standard and extended IP access lists on all interfaces are displayed.

**Configuration Examples**

```
Ruijie# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

## 1.41 show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.

**show ipv6 traffic-filter** [ **interface** *interface -name* ]

| Parameter Description | Parameter                              | Description    |
|-----------------------|----------------------------------------|----------------|
|                       | <b>interface</b> <i>Interface-name</i> | Interface name |

**Defaults** -

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.

**Configuration Examples** Ruijie# show ipv6 traffic-filter interface gigabitethernet 0/4

```
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/4.
```

## 1.42 show mac access-group

Use this command to display the MAC access list on the interface.

**show mac access-group** [ **interface** *interface* ]

| Parameter Description | Parameter                              | Description    |
|-----------------------|----------------------------------------|----------------|
|                       | <b>interface</b> <i>Interface-name</i> | Interface name |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the MAC access list configured on the interface. If no interface is specified, the MAC access lists on all interfaces are displayed.

**Configuration Examples** Ruijie# show mac access-group interface gigabitethernet 0/3

```
mac access-group mm in
Applied On interface GigabitEthernet 0/3.
```

## 1.43 show redirect interface

Use this command to display the access redirection configuration.

**show redirect [ interface *interface-name* ]**

| Parameter Description | Parameter                              | Description    |
|-----------------------|----------------------------------------|----------------|
|                       | <b>interface</b> <i>Interface-name</i> | Interface name |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the access redirection configuration on the interface. If no interface is specified, the access redirection configuration on all interfaces is displayed.

**Configuration** The following example displays the access redirection configuration on interface GigabitEthernet 0/3.

### Examples

```
Ruijie #show redirect interface gigabitEthernet 0/3
acl redirect configuration on interface gigabitEthernet 0/3
redirect destination interface gigabitEthernet 0/3 acl 1 in
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.44 svi router-acls enable

Use this command to enable the SVI filter only for the Layer3 packets. Use the **no** form of this command to disable this function.

**svi router-acls enable**

**no svi router-acls enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A.        |

**Defaults** The SVI filter takes effect for both Layer2 and Layer3 packets by default.

**Command mode** Global configuration mode

**Usage Guide** Use this command to make the SVI filter take effect only for the Layer3 packets,

**Configuration** The following example enables the SVI filter only for the Layer3 packets.

**Examples** Ruijie(config)#svi router-acls enable

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 2 QoS Commands

### 2.1 class

Use this command to add reference to an existing class map. Use the **no** form of this command to remove the class from the policy map.

**class** *class-map-name*

**no class** *class-map-name*

| Parameter   | Parameter             | Description               |
|-------------|-----------------------|---------------------------|
| Description | <i>class-map-name</i> | Reference to a class map. |

**Defaults** The function is disabled by default.

**Command** Policy configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example adds reference to the class map named cmap1.

**Examples**

```
Ruijie(config)# class-map cmap1
Ruijie(config-cmap)# match ip dscp 5
Ruijie(config-cmap)# exit
Ruijie(config)# policy-map pmap1
Ruijie(config-pmap)# class cmap1
Ruijie(config-pmap-c)# end
```

| Related Commands | Command                                                                                  | Description              |
|------------------|------------------------------------------------------------------------------------------|--------------------------|
|                  | <b>show policy-map</b> [ <i>policy-map-name</i> [ <b>class</b> <i>class-map-name</i> ] ] | Displays the policy map. |

**Platform** N/A

**Description**

### 2.2 class map

Use this command to create a class map and enter class-map configuration mode. Use the **no** or

**default** form of this command to remove a class map.

**class-map** *class-map-name*

**no class-map** *class-map-name*

**default class-map** *class-map-name*

| Parameter          | Parameter             | Description                                                           |
|--------------------|-----------------------|-----------------------------------------------------------------------|
| <b>Description</b> | <i>class-map-name</i> | Class map name. The class map name can be a maximum of 31 characters. |

**Defaults** None

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example creates a class map named `cm_acl` to match an access list named `me`.

**Examples**

```
Ruijie(config)# mac access-list extended me
Ruijie(config-ext-macl)# permit host 1111.2222.3333 any
Ruijie(config-ext-macl)# exit
Ruijie(config)# class-map cm_acl
Ruijie(config-cmap)# match access-group me
Ruijie(config-cmap)# exit
```

The following example creates a class map named `cm_dscp` to match DHCP 8, 16 and 24.

```
Ruijie(config)# class-map cm_dscp
Ruijie(config-cmap)# match ip dscp 8 16 24
Ruijie(config-cmap)# exit
```

## 2.3 drr-queue bandwidth

Use this command to set the DRR queue weight ratio. Use the **no** or **default** form of this command to restore the default setting.

**drr-queue bandwidth** *weight1...weight8*

**no drr-queue bandwidth**

**default drr-queue bandwidth**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |                          |                                                                                                                                                                                                                                                               |
|--------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <i>weight1...weight8</i> | 8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1.<br>For the products supporting the SP scheduling policy, the weight range is from 0 to 15.<br>For the products not supporting the SP scheduling policy, the weight range is from 1 to 15. |
|--------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Defaults** The default queue weight ratio is 1:1:1:1:1:1:1:1.

**Command Mode** Global configuration mode or interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the DRR queue weight ratio to 1:1:1:2:2:4:6:8.

**Examples**

```
Ruijie(config)# drr-queue bandwidth 1:1:1:2:2:4:6:8
```

**Related Commands**

| Command                     | Description                           |
|-----------------------------|---------------------------------------|
| <b>show mls qos queuing</b> | Displays information about the queue. |

**Platform** N/A

**Description**

## 2.4 match

Use this command to define a match criteria in class map configuration mode. Use the **no** form of this command to remove the match criteria.

```
match { access-group access_list | ip { dscp dscp-vlaue-list | precedence pre-vlaue-list } }
```

```
no match { access-group access_list | ip { dscp dscp-vlaue-list | precedence pre-vlaue-list } }
```

| Parameter          | Parameter                                  | Description                                                                                                                |
|--------------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <b>access-group</b> <i>access_list</i>     | Identifies a numbered or named access list as the match criteria.                                                          |
|                    | <b>ip dscp</b> <i>dscp-vlaue-list</i>      | Identifies DSCP values as the match criteria. Multiple DSCP can be configured. The range is from 0 to 63.                  |
|                    | <b>ip precedence</b> <i>pre-vlaue-list</i> | Identifies IP precedence values as the match criteria. Multiple IP precedence can be configured. The range is from 0 to 7. |

**Defaults** None

**Command Mode** Class map configuration mode

**Usage Guide** N/A



**Configuration** The following example creates a class map named cmap1 to match DSCP 20, 22, 24 and 30.

**Examples**

```
Ruijie(config)# class-map cmap1
Ruijie(config-cmap)# match ip dscp 20 22 24 30
```

**Related  
Commands**

| Command                                         | Description             |
|-------------------------------------------------|-------------------------|
| <b>show class-map</b> [ <i>class-map-name</i> ] | Displays the class map. |

**Platform** N/A

**Description**

## 2.5 mls qos cos

Use this command to configure the CoS value of an interface. Use the **no** form of this command to restore the default setting.

**mls qos cos** *default-cos*

**no mls qos cos**

| Parameter          | Parameter          | Description                                           |
|--------------------|--------------------|-------------------------------------------------------|
| <b>Description</b> | <i>default-cos</i> | CoS value of the interface. The range is from 0 to 7. |

**Defaults** The default CoS value is 0.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the default CoS value to 7.

**Examples**

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mls qos cos 7
```

| Related<br>Commands | Command                                           | Description                                      |
|---------------------|---------------------------------------------------|--------------------------------------------------|
|                     | <b>show mls qos interface</b> <i>interface-id</i> | Displays information of the specified interface. |

**Platform** N/A

**Description**

## 2.6 mls qos map cos-dscp

Use this command to map the CoS value to the DSCP value. Use the **no** or **default** form of this command to restore the default CoS-DSCP mapping.

**mls qos map cos-dscp** *dscp1...dscp8*

**no mls qos map cos-dscp**  
**default mls qos map cos-dscp**

| Parameter   | Parameter            | Description                                          |
|-------------|----------------------|------------------------------------------------------|
| Description | <i>dscp1...dscp8</i> | Specifies the DSCP value. The range is from 0 to 63. |

**Defaults** By default, the CoS 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples**

```
Ruijie(config)# mls qo map cos-dscp 8 10 16 18 24 26 32 34
```

| Related Commands | Command                           | Description                    |
|------------------|-----------------------------------|--------------------------------|
|                  | <b>show mls qos maps cos-dscp</b> | Displays the CoS-DSCP mapping. |

**Platform Description** N/A

## 2.7 mls qos map dscp-cos

Use this command to map the DSCP value to the CoS value. Use the **no** or **default** form of this command to restore the default DSCP-CoS mapping.

**mls qos map dscp-cos dscp-list to cos**  
**no mls qos map dscp-cos**  
**default mls qos map dscp-cos**

| Parameter   | Parameter        | Description                           |
|-------------|------------------|---------------------------------------|
| Description | <i>dscp-list</i> | DSCP list. The range is from 0 to 63. |
|             | <i>cos</i>       | CoS value. The range is from 0 to 7.  |

**Defaults** The default DSCP-CoS mapping is listed below:

|             |              |               |               |               |               |               |               |
|-------------|--------------|---------------|---------------|---------------|---------------|---------------|---------------|
| DSCP<br>0-7 | DSCP<br>8-15 | DSCP<br>16-23 | DSCP<br>24-31 | DSCP<br>32-39 | DSCP<br>40-47 | DSCP<br>48-55 | DSCP<br>56-63 |
| CoS 0       | CoS 1        | CoS 2         | CoS 3         | CoS 4         | CoS 5         | CoS 6         | CoS 7         |

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples**

```
Ruijie(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

| Related Commands | Command                           | Description                    |
|------------------|-----------------------------------|--------------------------------|
|                  | <b>show mls qos maps dscp-cos</b> | Displays the DSCP-CoS mapping. |

**Platform Description** N/A

## 2.8 mls qos map ip-precedence-dscp

Use this command to map the IP precedence to the DSCP value. Use the **no** or **default** form of this command to restore the default IP-precedence to DSCP mapping.

**mls qos map ip-precedence-dscp** *dscp1 ... dscp8*

**no mls qos map ip-precedence-dscp**

**default mls qos map ip-precedence-dscp**

| Parameter Description | Parameter            | Description                           |
|-----------------------|----------------------|---------------------------------------|
|                       | <i>dscp1...dscp8</i> | DSCP list. The range is from 0 to 63. |

**Defaults** By default, the IP precedence 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples**

```
Ruijie(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34
```

| Related Commands | Command                              | Description                                 |
|------------------|--------------------------------------|---------------------------------------------|
|                  | <b>show mls qos maps ip-pre-dscp</b> | Displays the IP-precedence to DSCP mapping. |

**Platform Description** N/A

## 2.9 mls qos scheduler

Use this command to configure the output queue scheduling. Use the **no** or **default** form of this command to restore the default scheduler.

**mls qos scheduler [ sp | rr | wrr | drr | wfq ]**

**no mls qos scheduler**

| Parameter   | Parameter  | Description                                                 |
|-------------|------------|-------------------------------------------------------------|
| Description | <b>sp</b>  | Specifies the absolute priority scheduling.                 |
|             | <b>rr</b>  | Specifies the round-robin scheduling.                       |
|             | <b>wrr</b> | Specifies the frame count weighted round-robin scheduling.  |
|             | <b>drr</b> | Specifies the frame length weighted round-robin scheduling. |
|             | <b>wfq</b> | Specifies the weighted fair queuing.                        |

**Defaults** The default queue scheduling is **wrr**.

**Command** Global configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example specifies the sp scheduling.

**Examples**

```
Ruijie(config)# mls qos scheduler sp
```

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)# mls qos scheduler drr
```

| Related  | Command                       | Description                           |
|----------|-------------------------------|---------------------------------------|
| Commands | <b>show mls qos scheduler</b> | Displays the output queue scheduling. |

**Platform** N/A

**Description**

## 2.10 mls qos trust

Use this command to configure the trust mode on an interface. Use the **no** or **default** form of this command to restore the default setting.

**mls qos trust { cos | dscp | ip-precedence }**

**no mls qos trust**

**default mls qos trust**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |                      |                                  |
|--------------------|----------------------|----------------------------------|
| <b>Description</b> | <b>cos</b>           | Specifies the CoS trust mode.    |
|                    | <b>dscp</b>          | Specifies the DSCP trust mode.   |
|                    | <b>ip-precedence</b> | Specifies the IP-PRE trust mode. |

**Defaults** No trust mode is configured by default.

**Command Mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the CoS trust mode.

**Examples**

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mls qos trust cos
```

| <b>Related Commands</b> | <b>Command</b>                                    | <b>Description</b>                              |
|-------------------------|---------------------------------------------------|-------------------------------------------------|
|                         | <b>show mls qos interface</b> <i>interface-id</i> | Displays the specified interface configuration. |

**Platform Description** N/A

## 2.11 police

Use this command to configure traffic policing for a class map in a policy map. Use the **no** form of this command to remove traffic policing for the class map.

```
police rate-bps burst-byte [exceed-action { drop | dscp new-dscp | cos new-cos [none-tos] }]
no police
```

| <b>Parameter Description</b> | <b>Parameter</b>            | <b>Description</b>                                                                                                                           |
|------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <i>rate-bps</i>             | Bandwidth limit value per second (The unit is KBits). This value depends on the specific product.                                            |
|                              | <i>burst-byte</i>           | Burst traffic limit value (The unit is KBytes). This value depends on the specific product.                                                  |
|                              | <b>drop</b>                 | Drops the packet. This is available only when the packet exceeds the bandwidth limit.                                                        |
|                              | <b>dscp</b> <i>new-dscp</i> | Modifies the DSCP value of the packet. This is available only when the packet exceeds bandwidth limit. The DSCP value range is from 0 to 63. |
|                              | <b>cos</b> <i>new-cos</i>   | Modifies the CoS value of the packet. This is available only when the packet exceeds bandwidth limit. The CoS value range is from 0 to 7.    |
|                              | <b>none-tos</b>             | Modifies the CoS value only.                                                                                                                 |

**Defaults** No traffic policing is configured for the class map by default.

**Command** Policy map class configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example configures traffic policing which modifies the DSCP value of the packet to 16 for class map “cm-acl” in policy map “pmap1”.

```
Ruijie(config)# policy-map pmap1
Ruijie(config-pmap)# class cm-acl
Ruijie(config-pmap-c)# police 102400 4096 exceed-action dscp 16
```

| Related Commands | Command                                                                                  | Description                            |
|------------------|------------------------------------------------------------------------------------------|----------------------------------------|
|                  | <b>show policy-map</b> [ <i>policy-map-name</i> [ <b>class</b> <i>class-map-name</i> ] ] | Displays the policy map configuration. |

**Platform** N/A  
**Description**

## 2.12 policy map

Use the following command to create a policy map and enter policy map configuration mode. Use the **no** or **default** form of this command to remove the specified policy map.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

**default policy-map** *policy-map-name*

| Parameter          | Parameter              | Description                                                             |
|--------------------|------------------------|-------------------------------------------------------------------------|
| <b>Description</b> | <i>policy-map-name</i> | Policy map name. The policy map name can be a maximum of 31 characters. |

**Defaults** No policy map is configured by default.

**Command** Global configuration mode.  
**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example creates policy map “po”, and then adds a reference to class map “cmap1”. Sets the rate limit value to 10 Mbps, the burst traffic limit value to 256 Kbps, and discard packets which exceed the limit.

```
Ruijie(config)# policy-map po
Ruijie(config-pmap)# class cmaplRuijie(config-pmap-c)# police 10240 256
exceed-action drop
```

| Related  | Command                                                                                  | Description                            |
|----------|------------------------------------------------------------------------------------------|----------------------------------------|
| Commands | <b>show policy-map</b> [ <i>policy-map-name</i> [ <b>class</b> <i>class-map-name</i> ] ] | Displays the policy map configuration. |

**Platform** N/A

**Description**

## 2.13 priority-queue

Use this command to configure the output queue scheduling policy to SP. Use the **no** or **default** form of this command to restore the default queue scheduling policy.

**priority-queue**

**no priority-queue**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** The default output queue scheduling policy is WRR.

**Command Mode** Global configuration mode.

**Usage Guide** This command shares the same configuration with the **mls qos scheduler sp**. The **show run** command displays this configuration in the **mls qos scheduler sp** item instead of **priority-queue**.

**Configuration Examples** The following example configures the output queue scheduling policy to SP.

```
Ruijie(config)# priority-queue
```

| Related  | Command                       | Description                                  |
|----------|-------------------------------|----------------------------------------------|
| Commands | <b>show mls qos scheduler</b> | Displays the output queue scheduling policy. |

**Platform** N/A

**Description**

## 2.14 priority-queue cos-map

Use this command to configure the mapping between the CoS value and the queue ID. Use the **no** or **default** form of this command to restore the default CoS mapping to the queue.





|                                                                                |                                                                                                                     |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
|                                                                                | interface bandwidth to the queue on the device supporting both unicast and multicast queue bandwidth configuration. |
| <i>queue-id</i>                                                                | Queue ID. The range is from 1 to 8.                                                                                 |
| <b>bandwidth</b><br>{ <b>minimum</b>  <br><b>maximum</b> }<br><i>bandwidth</i> | Bandwidth value. The value range depends on the specific product.                                                   |

**Defaults** No minimum or maximum of interface bandwidth to a queue is configured by default.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the minimum interface bandwidth of unicast queue 1 to 5 Mbps, and the maximum to 10 Mbps.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# qos queue ucast 1 bandwidth maximum
10240
Ruijie(config-if-GigabitEthernet 0/1)# qos queue ucast 1 bandwidth minimum
5120
```

The following example configures the minimum interface bandwidth of unicast queue 2 to 2 Mbps.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# qos queue ucast 2 bandwidth minimum
2048
```

The following example configures minimum interface bandwidth of multicast queue 1 to 1 Mbps, and the maximum to 5 Mbps.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# qos queue mcast 1 bandwidth maximum
5120
Ruijie(config-if-GigabitEthernet 0/1)# qos queue mcast 1 bandwidth minimum
1024
```

| Related Commands | Command                                                          | Description                                    |
|------------------|------------------------------------------------------------------|------------------------------------------------|
|                  | <b>show qos bandwidth [ interfaces<br/><i>interface-id</i> ]</b> | Displays the interface bandwidth of the queue. |

**Platform** N/A

## Description

## 2.16 queueing wred

Use this command to enable the WRED (Weighted Random Early Detection) function. Use the **no** or **default** form of this command to disable the WRED function.

**queueing wred**

**no queueing wred**

**default queueing wred**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** WRED is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables WRED.

```
Ruijie(config)# queueing wred
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 2.17 rate-limit

Use this command to configure rate limiting on the interface. Use the **no** or **default** form of this command to remove rate limiting from the interface.

**rate-limit { input | output } *bps burst-size***

**no rate-limit { input | output }**

**default rate-limit { input | output }**

| Parameter   | Parameter     | Description                                                                                       |
|-------------|---------------|---------------------------------------------------------------------------------------------------|
| Description | <b>input</b>  | Configures input rate limiting.                                                                   |
|             | <b>output</b> | Configures output rate limiting.                                                                  |
|             | <i>bps</i>    | Bandwidth limit value per second (The unit is KBits). This value depends on the specific product. |

|                   |                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------|
| <i>burst-size</i> | Burst traffic limit value (The unit is KBytes). This value depends on the specific product. |
|-------------------|---------------------------------------------------------------------------------------------|

**Defaults** Rate limiting is not configured by default.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate limit value to 10 Mbps, and the burst traffic limit value to 256 Kbps.

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# rate-limit input 10240 256
```

| Related Commands | Command                                                          | Description                                                |
|------------------|------------------------------------------------------------------|------------------------------------------------------------|
|                  | <b>show mls qos rate-limit [ interface <i>interface-id</i> ]</b> | Displays the rate limiting configuration of the interface. |

**Platform** N/A

**Description**

## 2.18 service-policy

Use this command to apply the policy map to the interface, the virtual group or globally. Use the **no** or **default** form of this command to remove the policy map.

**service-policy** { **input** | **output** } *policy-map-name*

**no service-policy** { **input** | **output** } *policy-map-name*

**default service-policy** { **input** | **output** } *policy-map-name*

| Parameter          | Parameter              | Description                                     |
|--------------------|------------------------|-------------------------------------------------|
| <b>Description</b> | <i>policy-map-name</i> | Policy map name                                 |
|                    | <b>input</b>           | Applies the policy map to the input direction.  |
|                    | <b>output</b>          | Applies the policy map to the output direction. |

**Defaults** No policy map is configured on the interface or virtual group by default.

**Command** Interface configuration mode, and virtual group configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example applies policy map “po” to the input direction of interface GigabitEthernet 1/3.

**Examples**

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# service-policy input po
```

The following example applies policy map “po” to the output direction of virtual group 3.

```
Ruijie(config)# virtual-group 3
Ruijie(config-VirtualGroup)# service-policy output po
```

**Related Commands**

| Command                                    | Description                                                 |
|--------------------------------------------|-------------------------------------------------------------|
| <b>show mls qos interface policers</b>     | Displays the policy map configuration on the interface.     |
| <b>show mls qos virtual-group policers</b> | Displays the policy map configuration on the virtual group. |

**Platform**

N/A

**Description**

## 2.19 set

Use this command to configure the CoS, DSCP or VID value for the traffic. Use the **no** form of this command to remove the CoS, DSCP or VID value from the traffic.

**set { ip dscp *new-dscp* | cos *new-cos* [ none-tos ] | vid *new-vid* }**

**no set { ip dscp | cos | vid }**

**Parameter**

| Parameter                      | Description                                                            |
|--------------------------------|------------------------------------------------------------------------|
| <b>ip dscp <i>new-dscp</i></b> | Configures the DSCP value for the traffic. The range is from 0 to 63.  |
| <b>cos <i>new-cos</i></b>      | Configures the CoS value for the traffic. The range is from 0 to 7.    |
| <b>none-tos</b>                | Configures the CoS value only.                                         |
| <b>vid <i>new-vid</i></b>      | Configures the VID value for the traffic. The range is from 1 to 4094. |

**Defaults**

No CoS, DSCP or VID value is configured for the traffic in policy map class mode.

**Command**

Policy map class configuration mode

**Mode****Usage Guide**

N/A

**Configuration** The following example creates policy map “pmap1”, and adds a reference to class map “cmap1”.

**Examples**

```
Ruijie(config)# policy-map pmap1
Ruijie(config-pmap)# class cmap1
```

The following example modifies the CoS value of the traffic to 3.

```
Ruijie(config-pmap-c)# set cos 3
```

| Related Commands | Command                                                                                               | Description                                             |
|------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
|                  | <b>show</b><br><b>policy-map</b> [ <i>policy-map-name</i><br>[ <b>class</b> <i>class-map-name</i> ] ] | Displays the policy map configuration on the interface. |

**Platform** N/A

**Description**

## 2.20 show class-map

Use this command to display the class map.

```
show class-map [class-map-name]
```

| Parameter          | Parameter             | Description     |
|--------------------|-----------------------|-----------------|
| <b>Description</b> | <i>class-map-name</i> | Class map name. |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all class maps.

**Examples**

```
Ruijie# show class-map

Class Map cmap1
 Match ip dscp 20 40
Class Map cmap2
 Match access-group 110
```

The fields in the output of this command are described in the following table.

| Field     | Description                   |
|-----------|-------------------------------|
| Class Map | Indicates the class map name. |
| Match     | Indicates the matched rule.   |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 2.21 show mls qos interface

Use this command to display the QoS configuration of the interface.

**show mls qos interface** [ *interface-id* ] [ **policers** ]

| Parameter          | Parameter           | Description                                                |
|--------------------|---------------------|------------------------------------------------------------|
| <b>Description</b> | <i>interface-id</i> | Interface name                                             |
|                    | <b>policers</b>     | Displays the traffic policing configured on the interface. |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the QoS configuration of interface GigabitEthernet 1/3.

```
Ruijie# show mls qos interface gigabitethernet 1/3
Interface: GigabitEthernet 0/3
Ratelimit input: 10240 256
Ratelimit output: 51200 4096
Attached input policy-map: pmap1
Attached output policy-map:
Default trust: dscp
Default cos: 3
Scheduler type: drr
Wrr queue bandwidth: 1 1 1 1 2 2 2 2
Drr queue bandwidth: 1 1 2 2 2 2 4 4
Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

The fields in the output of this command are described in the following table.

| Field                      | Description                             |
|----------------------------|-----------------------------------------|
| Interface                  | Indicates the interface name.           |
| Ratelimit input            | Indicates the input rate limit value .  |
| Ratelimit output           | Indicates the output rate limit value . |
| Attached input policy-map  | Indicates the input policy map .        |
| Attached output policy-map | Indicates the output policy map.        |

|               |                                            |
|---------------|--------------------------------------------|
| Default trust | Indicates the trust mode of the interface. |
| Default cos   | Indicates the default CoS value.           |

The following example displays the QoS configuration of all interfaces.

```
Ruijie# show mls qos interface policers
Interface: GigabitEthernet 0/1
Attached input policy-map: pmap1
Attached output policy-map: pmap1
Interface: GigabitEthernet 0/2
Attached input policy-map: p1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 2.22 show mls qos maps

Use this command to display DSCP-CoS mapping, CoS-DSCP mapping and IP-PRE-DSCP mapping.

**show mls qos maps [ cos-dscp | dscp-cos | ip-prec-dscp ]**

| Parameter          | Parameter           | Description                        |
|--------------------|---------------------|------------------------------------|
| <b>Description</b> | <b>cos-dscp</b>     | Displays the CoS-DSCP mapping.     |
|                    | <b>dscp-cos</b>     | Displays the DSCP-CoS mapping.     |
|                    | <b>ip-prec-dscp</b> | Displays the IP-PRE-DSCP mapping.. |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the CoS-DSCP mapping.

```
Ruijie# show mls qos maps cos-dscp
cos dscp
--- ----
0 0
```

```

1 8
2 16
3 24
4 32
5 40
6 48
7 56

```

The fields in the output of this command are described in the following table.

| Field | Description                       |
|-------|-----------------------------------|
| cos   | Indicates the CoS value.          |
| dscp  | Indicates the DSCP value mapped . |

The following example displays the DSCP- CoS mapping.

```

Ruijie# show mls qos maps dscp-cos
dscp cos dscp cos dscp cos dscp cos

0 0 1 0 2 0 3 0
4 0 5 0 6 0 7 0
8 1 9 1 10 1 11 1
12 1 13 1 14 1 15 1
16 2 17 2 18 2 19 2
20 2 21 2 22 2 23 2
24 3 25 3 26 3 27 3
28 3 29 3 30 3 31 3
32 4 33 4 34 4 35 4
36 4 37 4 38 4 39 4
40 5 41 5 42 5 43 5
44 5 45 5 46 5 47 5
48 6 49 6 50 6 51 6
52 6 53 6 54 6 55 6
56 7 57 7 58 7 59 7
60 7 61 7 62 7 63 7

```

The fields in the output of this command are described in the following table.

| Field | Description |
|-------|-------------|
|-------|-------------|



|      |                                  |
|------|----------------------------------|
| dscp | Indicates the DSCP value.        |
| cos  | Indicates the CoS value mapped . |

The following example displays the IP-PRE-DSCP mapping.

```
Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp

0 0
1 8
2 16
3 24
4 32
5 40
6 48
7 56
```

The fields in the output of this command are described in the following table.

| Field         | Description                       |
|---------------|-----------------------------------|
| ip-precedence | Indicates the IP-PRE value.       |
| dscp          | Indicates the DSCP value mapped . |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |
| Platform         | N/A     |             |
| Description      |         |             |

## 2.23 show mls qos queueing

Use this command to display the QoS queueing configuration.

**show mls qos queueing** [ interface *interface-id* ]

| Parameter    | Parameter                                                                      | Description      |
|--------------|--------------------------------------------------------------------------------|------------------|
| Description  | interface <i>interface-id</i>                                                  | ID of interface. |
| Defaults     | N/A                                                                            |                  |
| Command Mode | Privileged EXEC mode, global configuration mode, interface configuration mode. |                  |

**Usage Guide** N/A

**Configuration** The following example displays the QoS queuing configuration.

**Examples**

```
Ruijie# show mls qos queueing
```

```
Cos-queue map:
```

```
cos qid
```

```
--- ---
```

```
0 1
```

```
1 2
```

```
2 3
```

```
3 4
```

```
4 5
```

```
5 6
```

```
6 7
```

```
7 8
```

```
wrr bandwidth weights:
```

```
qid weights
```

```
--- -----
```

```
1 1
```

```
2 2
```

```
3 3
```

```
4 4
```

```
5 5
```

```
6 6
```

```
7 7
```

```
8 8
```

```
drp bandwidth weights:
```

```
qid weights
```

```
--- -----
```

```
1 3
```

```
2 3
```

```
3 3
```

```

4 3
5 3
6 3
7 3
8 3

wfq bandwidth weights:
qid weights

1 3
2 4
3 5
4 6
5 7
6 8
7 9
8 10

Interface: GigabitEthernet 0/1

Wrr queue bandwidth: 1 1 1 1 2 2 2 2
Drr queue bandwidth: 1 1 2 2 2 2 4 4
Wfq queue bandwidth: 1 1 2 2 4 4 4 4

```

The fields in the output of this command are described in the following table.

| Field                 | Description                                                   |
|-----------------------|---------------------------------------------------------------|
| Cos-queue map         | Indicates the mapping between the CoS value and the queue ID. |
| wrr bandwidth weights | Indicates the WRR queue weight.                               |
| drr bandwidth weights | Indicates the DRR queue weight.                               |
| wfq bandwidth weights | Indicates the WFQ queue weight.                               |
| cos                   | Indicates the CoS value.                                      |
| qid                   | Indicates the queue ID.                                       |
| weights               | Indicates the weight value                                    |

```

Ruijie# show mls qos queueing interface gigabitEthernet 0/1

Interface: GigabitEthernet 0/1

Wrr queue bandwidth: 1 1 1 1 2 2 2 2

```

```

Drr queue bandwidth: 1 1 2 2 2 2 4 4
Wfq queue bandwidth: 1 1 2 2 4 4 4 4

```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 2.24 show mls qos rate-limit

Use this command to display the rate limiting configuration of the interface.

**show mls qos rate-limit [ interface *interface-id* ]**

| Parameter          | Parameter           | Description    |
|--------------------|---------------------|----------------|
| <b>Description</b> | <i>interface-id</i> | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the rate limiting configuration of all interfaces.

```

Ruijie# show mls qos rate-limit

Interface: GigabitEthernet 0/1
 rate limit input Kbps = 10240 burst = 256

Interface: GigabitEthernet 0/3
 rate limit output Kbps = 102400 burst = 4096

```

The fields in the output of this command are described in the following table.

| Field                                | Description                                                                      |
|--------------------------------------|----------------------------------------------------------------------------------|
| Interface                            | Indicates the interface name.                                                    |
| rate limit input Kbps = x burst = y  | Indicates the input rate limit value, and the input burst traffic limit value.   |
| rate limit output Kbps = x burst = y | Indicates the output rate limit value, and the output burst traffic limit value. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 2.25 show mls qos scheduler

Use this command to display the queue scheduling policy.

**show mls qos scheduler** [ **interface** *interface-id* ]

| Parameter          | Parameter                            | Description          |
|--------------------|--------------------------------------|----------------------|
| <b>Description</b> | <b>interface</b> <i>interface-id</i> | ID of the interface. |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the queue scheduling policy.

```
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
 Weighted Round Robin
Interface GigabitEthernet 0/1 Multi-Layer Switching scheduling:
 Deficit Round Robin
```

The fields in the output of this command are described in the following table.

| Field                | Description                                                                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Weighted Round Robin | Indicates that the queue scheduling policy is WRR.<br>The other queue scheduling policies are listed as follows:<br>SP: Strict Priority<br>RR: Round Robin<br>DRR: Deficit Round Robin<br>WFQ: Weighted Fair Queue |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 2.26 show mls qos virtual-group

Use this command to display the policy map configuration on the virtual group.

**show mls qos virtual-group** [ *virtual-group-number* | **policers** ]

| Parameter   | Parameter                   | Description                                                  |
|-------------|-----------------------------|--------------------------------------------------------------|
| Description | <i>virtual-group-number</i> | Virtual group number. The range is from 1 to 128.            |
|             | <b>policers</b>             | Displays the policy map configuration on all virtual groups. |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the policy map configuration on all virtual groups.

```
Ruijie# show mls qos virtual-group policers
Virtual-group: 1
Attached input policy-map: pmap1
Virtual-group: 20
Attached output policy-map: pmap2
```

The fields in the output of this command are described in the following table.

| Field                      | Description                                                   |
|----------------------------|---------------------------------------------------------------|
| Virtual-group              | Indicates the virtual group number.                           |
| Attached input policy-map  | Indicates the policy map applied on the input virtual group.  |
| Attached output policy-map | Indicates the policy map applied on the output virtual group. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 2.27 show policy-map

Use this command to display policy maps.

**show policy-map** [ *policy-map-name* [ **class** *class-map-name* ] ]

| Parameter   | Parameter              | Description     |
|-------------|------------------------|-----------------|
| Description | <i>policy-map-name</i> | Policy map name |
|             | <i>class-map-name</i>  | Class map name  |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays configuration of policy map "pmap1".

```
Ruijie# show policy-map pmap1

Policy Map pmap1
 Class cmap1
 set ip dscp 16
 Class cmap2
 police 10240 256 exceed-action dscp 8
 Class cmap3
 police 512000 4096 exceed-action drop
```

The fields in the output of this command are described in the following table.

| Field      | Description                                                                             |
|------------|-----------------------------------------------------------------------------------------|
| Policy Map | Indicates the policy map name.                                                          |
| Class      | Indicates the class map name.                                                           |
| set        | Indicates that the DSCP value is modified in this example.                              |
| police     | Indicates bandwidth limit configuration and the action policy for the violated packets. |

The following example displays the action policy for the traffic of class map "cmap1" in policy map "pmap1".

```
Ruijie#show policy-map pmap1 class cmap1
Class cmap1
set ip dscp 16
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 2.28 show qos bandwidth

Use this command to display the bandwidth configuration.

**show qos bandwidth [ interfaces *interface-id* ]**

| Parameter          | Parameter           | Description    |
|--------------------|---------------------|----------------|
| <b>Description</b> | <i>interface-id</i> | Interface name |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the bandwidth configuration of interface GigabitEthernet 0/1. (Taking the device supporting the bandwidth configuration of the unicast queue or the multicast queue for example.)

```
Ruijie# show qos bandwidth interface gigabitEthernet 0/1

Interface: GigabitEthernet 0/1

uc-queue-id | minimum-bandwidth | maximum-bandwidth

1 5120 10240
2 0 0
3 0 0
4 0 0
5 0 0
```



```

 6 0 0
 7 0 0
 8 0 0

Total ucast-queue minimum-bandwidth: 5120
Total ucast-queue maximum-bandwidth: 10240

Interface: GigabitEthernet 0/1

mc-queue-id | minimum-bandwidth | maximum-bandwidth

 1 1024 5120
 2 0 0
 3 0 0
 4 0 2048

Total mcast-queue minimum-bandwidth: 1024
Total mcast-queue maximum-bandwidth: 5120

```

The fields in the output of this command are described in the following table.

| Field                                                                      | Description                                                                                                |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Interface                                                                  | Indicates the interface name.                                                                              |
| queue-id                                                                   | Indicates the queue ID.                                                                                    |
| uc-queue-id                                                                | Indicates the unicast queue ID.                                                                            |
| mc-queue-id                                                                | Indicates the multicast queue ID.                                                                          |
| minimum-bandwidth                                                          | Indicates the minimum bandwidth configuration. The unit is Kbps.                                           |
| maximum-bandwidth                                                          | Indicates the maximum bandwidth configuration. The unit is Kbps.                                           |
| Total queue minimum-bandwidth<br>Total queue maximum-bandwidth             | Indicates the total bandwidth of minimum and maximum when both unicast and multicast queues are displayed. |
| Total ucast-queue minimum-bandwidth<br>Total ucast-queue maximum-bandwidth | Indicates the total bandwidth of minimum and maximum when only unicast queue is displayed.                 |
| Total mcast-queue minimum-bandwidth<br>Total mcast-queue maximum-bandwidth | Indicates the total bandwidth of minimum and maximum when only multicast queue is displayed.               |

|                         |                |                    |
|-------------------------|----------------|--------------------|
| <b>Related Commands</b> | <b>Command</b> | <b>Description</b> |
|                         | N/A            | N/A                |

**Platform** N/A  
**Description**

## 2.29 show queueing wred interface

Use this command to display WRED settings on the interface.

**show queueing wred interface** *interface-id*

|                              |                     |                    |
|------------------------------|---------------------|--------------------|
| <b>Parameter Description</b> | <b>Parameter</b>    | <b>Description</b> |
|                              | <i>interface-id</i> | Interface name     |

**Defaults** None

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the WRED settings on interface GigabitEthernet 1/3.

```
Ruijie# show queueing wred interface gigabitethernet 1/3

qid max_1 min_1 prob_1 max_2 min_2 prob_2

1 100 30 100 100 70 100
2 100 60 100 100 30 100
3 100 80 30 100 30 40
4 100 80 100 100 100 100
5 100 80 100 100 100 100
6 100 80 100 100 100 100
7 100 80 100 100 100 100
8 100 80 100 100 100 100
```

```

cos qid threshold_id

0 1 1
1 2 2
2 3 2
3 4 2
4 5 2
5 6 1
6 7 1
7 8 1

```

The fields in the output of this command are described in the following table.

| Field                  | Description                                                        |
|------------------------|--------------------------------------------------------------------|
| qid                    | Indicates the queue ID.                                            |
| max_x                  | Indicates the upper threshold of the x group.                      |
| min_x                  | Indicates the lower threshold of the x group.                      |
| prob_x                 | Indicates the maximum probability of being dropped of the x group. |
| cos  qid  threshold_id | Indicates the mapping of CoS value, queue ID and threshold number. |

#### Related Commands

| Command | Description |
|---------|-------------|
| N/A.    | N/A.        |

#### Platform Description

N/A.

## 2.30 show virtual-group

Use this command to display the member port in the virtual group.

**show virtual-group** [ *virtual-group-number* | **summary** ]

#### Parameter Description

| Parameter                   | Description                                       |
|-----------------------------|---------------------------------------------------|
| <i>virtual-group-number</i> | Virtual group number. The range is from 1 to 128. |
| <b>summary</b>              | Displays the member port in all virtual groups.   |

|                     |                                                                                |
|---------------------|--------------------------------------------------------------------------------|
| <b>Defaults</b>     | N/A                                                                            |
| <b>Command Mode</b> | Privileged EXEC mode, global configuration mode, interface configuration mode. |
| <b>Usage Guide</b>  | N/A                                                                            |

**Configuration Examples** The following example displays the member port in all virtual groups.

**Examples**

```
Ruijie# show virtual-group summary

virtual-group member

1 Gi0/1 Gi0/2
2 Gi0/0
```

The fields in the output of this command are described in the following table.

| Field         | Description                                     |
|---------------|-------------------------------------------------|
| virtual-group | Indicates the virtual group number.             |
| member        | Indicates the member port in the virtual group. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 2.31 virtual-group

Use this command to create a virtual group in global configuration mode.

Use this command to configure add an interface to a virtual group in interface configuration mode.

Use the **no** or **default** form of this command to remove a virtual group in global configuration mode.

Use the **no** or **default** form of this command to remove an interface from a virtual group in interface configuration mode.

**virtual-group** *virtual-group-number*

**no virtual-group** *virtual-group-number*

**default virtual-group** *virtual-group-number*

| Parameter Description | Parameter                   | Description                                       |
|-----------------------|-----------------------------|---------------------------------------------------|
|                       | <i>virtual-group-number</i> | Virtual group number. The range is from 1 to 128. |

**Defaults** No virtual group is configured, or no interface is added to a virtual group, by default.

**Command Mode** Interface configuration mode, global configuration mode.

**Usage Guide** The member port added to the virtual group must be a physical port or an aggregate port member. The member ports of a virtual group must be on the same module of a chassis switch or on the same box switch.

**Configuration Examples** The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3:

```
Ruijie(config)# interface gigabitEthernet 1/3
Ruijie(config-if)# virtual-group 3
```

**Related Commands**

| Command                                                                       | Description                               |
|-------------------------------------------------------------------------------|-------------------------------------------|
| <b>show virtual-group</b> [ <i>virtual-group-number</i> ]<br><b>summary</b> ] | Displays the virtual group configuration. |

**Platform Description** N/A

## 2.32 wfq-queue bandwidth

Use this command to configure the WFQ queue weight ratio. Use the **no** or **default** form of this command to restore the default setting.

**wfq-queue bandwidth** *weight1 ... weight8*

**no wfq-queue bandwidth**

**default wfq-queue bandwidth**

**Parameter Description**

| Parameter                | Description                                                                                                                                                                                                                                             |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>weight1...weight8</i> | 8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15. |

**Defaults** The default queue weight ratio is 1:1:1:1:1:1:1:1.

**Command Mode** Global configuration mode.

**Usage Guide** If the weight value is 0, the SP scheduling policy is applied.

**Configuration** The following example configures the WFQ queue weight ratio to 1:1:2:4:4:4:6:8.

**Examples**

```
Ruijie(config)# wfq-queue bandwidth 1 1 2 4 4 4 6 8
```

**Related  
Commands**

| Command                      | Description                             |
|------------------------------|-----------------------------------------|
| <b>show mls qos queueing</b> | Displays the QoS queuing configuration. |

**Platform** N/A**Description**

## 2.33 wrr-queue bandwidth

Use this command to set the WRR weight ratio. Use the **no** or **default** form of this command to restore the default setting.

**wrr-queue bandwidth** *weight1 ... weight8*

**no wrr-queue bandwidth**

**default wrr-queue bandwidth**

**Parameter****Description**

| Parameter                | Description                                                                                                                                                                                                                                             |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>weight1...weight8</i> | 8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15. |

**Defaults** The default queue weight ratio is 1:1:1:1:1:1:1:1.**Command** Global configuration mode**Mode****Usage Guide** If the weight value is 0, the SP scheduling policy is applied.**Configuration** The following example configures the WRR queue weight ratio to 1:1:1:1:2:2:4:8.**Examples**

```
Ruijie(config)# wrr-queue bandwidth 1 1 1 1 2 2 4 8
```

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)# wrr-queue bandwidth 1 1 2 2 2 2 4 4
```

**Related  
Commands**

| Command                      | Description                             |
|------------------------------|-----------------------------------------|
| <b>show mls qos queueing</b> | Displays the QoS queuing configuration. |

**Platform** N/A**Description**

## 2.34 wrr-queue cos-map

Use this command to map the CoS value to a threshold for a specified queue. Use the **no** or **default** form of this command to restore the default settings

**wrr-queue cos-map** *threshold\_id* *cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]]

**no wrr-queue cos-map** *threshold\_id*

**default wrr-queue cos-map** *threshold\_id*

| Parameter Description | Parameter           | Description                                                                               |
|-----------------------|---------------------|-------------------------------------------------------------------------------------------|
|                       | <i>threshold_id</i> | Threshold number. The range is from 1 to 2. Up to two threshold values can be configured. |
|                       | <i>cos_N</i>        | CoS value. The range is from 0 to 7. Up to 8 CoS values can be configured.                |

**Defaults** All CoS values are mapped to the threshold 1.

**Command mode** Interface configuration mode.

**Usage Guide** DSCP-threshold mapping can be enabled by mapping DSCP-CoS to CoS-threshold. When all CoS values are mapped to one threshold on the interface, it changes the enabled WRED to RED.

**Configuration Examples** The following example enters the interface GigabitEthernet 1/3 to map CoS 1, 2 to threshold 2.

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)#wrr-queue cos-map 2 1 6
```

| Related Commands | Command                                                 | Description                                       |
|------------------|---------------------------------------------------------|---------------------------------------------------|
|                  | <b>show queueing wred interface</b> <i>interface-id</i> | Displays the WRED configuration on the interface. |

**Platform Description** N/A.

## 2.35 wrr-queue random-detect min-threshold

Use this command to configure the minimum WRED drop threshold. Use the **no** or **default** form of this command to restore the default WRED drop threshold.

**wrr-queue random-detect min-threshold** *queue\_id* *thr1* [*thr2*]

**no wrr-queue random-detect min-threshold** *queue\_id*  
**default wrr-queue random-detect min-threshold** *queue\_id*

**Parameter  
Description**

| Parameter       | Description                                                                               |
|-----------------|-------------------------------------------------------------------------------------------|
| <i>queue_id</i> | Queue ID.                                                                                 |
| <i>thrN</i>     | Up to two threshold values can be configured. The threshold value range is from 1 to 100. |

**Defaults**

Two threshold values are configured, and the default threshold values are 100 and 80.

**Command  
mode**

Interface configuration mode.

**Usage Guide**

N/A

**Configuration  
Examples**

The following example configures the low WRED drop thresholds to 60 and 70 for queue 1.

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# wrr-queuerandom-detect min-threshold
1 60 70
```

**Related  
Commands**

| Command                                                | Description                                       |
|--------------------------------------------------------|---------------------------------------------------|
| <b>show queuing wred interface</b> <i>interface-id</i> | Displays the WRED configuration on the interface. |

**Platform  
Description**

N/A.

## 2.36 wrr-queue random-detect probability

Use this command to configure the WRED packet drop probability. Use the **no** or **default** form of this command to restore the WRED packet drop probability.

**wrr-queue random-detect probability** *queue\_id* *prob1* [ *prob2* ]  
**no wrr-queue random-detect probability** *queue\_id*  
**default wrr-queue random-detect probability** *queue\_id*

**Parameter  
Description**

| Parameter       | Description                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------|
| <i>queue_id</i> | Queue ID.                                                                                   |
| <i>proN</i>     | Up to two probability values can be configured. The threshold value range is from 1 to 100. |



**Defaults** Two packet drop probability values are configured, and the default probability values are 100 and 80.

**Command mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the WRED packet drop values to 50 and 70 for queue 1.

**Examples**

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# wrr-queue random-detect probability 1
50 70
```

**Related Commands**

| Command                                                 | Description                                       |
|---------------------------------------------------------|---------------------------------------------------|
| <b>show queueing wred interface</b> <i>interface-id</i> | Displays the WRED configuration on the interface. |

**Platform Description** N/A.



## Reliability Configuration Commands

---

1. REUP Commands
2. RLDP Commands
3. DLDP Commands
4. PCAP Commands
5. VRRP Commands
6. VRRP Plus Commands
7. BFD Commands
8. IP Event Dampening Commands
9. VSU Commands
10. RNS&Track Commands
11. VSD Commands
12. NLB Group Commands

# 1 REUP Commands

## 1.1 link state group

Use this command to add the port into the specified link state track group. The **no** form of this command is used to delete a port from the specified link state track group.

**link state group** *num* { **upstream** | **downstream** }

**no link state group**

| Parameter Description | Parameter         | Description                                                                |
|-----------------------|-------------------|----------------------------------------------------------------------------|
|                       | <i>num</i>        | ID of the link state track group.                                          |
|                       | <b>upstream</b>   | Configures the port to be an upstream port in the link state track group.  |
|                       | <b>downstream</b> | Configures the port to be a downstream port in the link state track group. |

**Defaults** The port is not added into any link state track group.

**Command Mode** Interface configuration mode.

**Usage Guide** First create a link state track group and then add a port into the specified link state track group.

**Configuration Examples** The following example shows how to add the port fa0/2 into the link state track group:

```
Ruijie(config)# link state track 1
Ruijie(config)# interface fa 0/2
Ruijie(config-if)# link state group 1 upstream
```

| Related Commands | Command                 | Description                       |
|------------------|-------------------------|-----------------------------------|
|                  | <b>link state track</b> | Enables a link state track group. |

**Platform Description** N/A.

## 1.2 link state track

Use this command to enable the link state track group. The **no** form of this command is used to disable a link state track group

**link state track** [ *num* ]

**no link state track** [ *num* ]

| Parameter Description | Parameter  | Description                                 |
|-----------------------|------------|---------------------------------------------|
|                       | <i>num</i> | Interface ID of the link aggregation group. |

**Defaults** N/A.

**Command Mode** Global configuration mode.

**Mode**

**Usage Guide** First create a link state track group and then add a port into the specified link state track group.

**Configuration** The following example shows how to create a link state track group:

**Examples** Ruijie(config)# link state track 1

| Related Commands | Command                 | Description                                            |
|------------------|-------------------------|--------------------------------------------------------|
|                  | <b>link state group</b> | Adds the port to the specified link state track group. |

**Platform** N/A.

**Description**

### 1.3 mac-address-table move update max-update-rate

Use this command to configure the maximum number of MAC address update packets sent per second.

**mac-address-table move update max-update-rate** *pkts-per-second*

**no mac-address-table move update max-update-rate**

| Parameter Description | Parameter              | Description                                                                                                                |
|-----------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------|
|                       | <i>pkts-per-second</i> | The maximum number of MAC address update packets sent per second. It ranges from 0 to 32000, and the default value is 150. |

**Defaults** A maximum of 150 MAC address update packets are sent per second.

**Command Mode** Global configuration mode.

**Mode**

**Usage Guide** When a link is switched, REUP sends a certain number of MAC address update packets to an uplink device in every second to recover downlink data transmission of the uplink device.

**Configuration** The following example shows how to configure the maximum number of MAC address update packets sent per second:

**Examples**

```
Ruijie(config)# mac-address-table move update max-update-rate 20
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A.    | N/A.        |

**Platform**

N/A.

**Description**

## 1.4 mac-address-table move update receive

Use this command to enable REUP to receive the mac-address-table update messages.

**mac-address-table move update receive**

**no mac-address-table move update receive**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A.      | N/A.        |

**Defaults**

Disabled.

**Command Mode**

Global configuration mode.

**Usage Guide**

The dual link backup switchover will lead to the loss of downstream data flow, for the MAC address for the uplink switch has not been updated in time. Therefore, it is necessary to update the MAC address table of the uplink switch, to reduce the loss of L2 data flow. You need to enable the switch of receiving the MAC address update messages on the uplink switch.

**Configuration Examples**

```
Ruijie(config)# mac-address-table move update receive
```

**Related Commands**

| Command                                      | Description                                                     |
|----------------------------------------------|-----------------------------------------------------------------|
| <b>mac-address-table move update transit</b> | Enables REUP to transmit the mac-address-table update messages. |

**Platform**

N/A.

**Description**

## 1.5 mac-address-table move update receive vlan

Use this command to configure the VLANs processing MAC address update packets.

**mac-address-table move update receive vlan** *vlan-range*

**no mac-address-table move update receive vlan** *vlan-range*

| Parameter Description | Parameter         | Description                                               |
|-----------------------|-------------------|-----------------------------------------------------------|
|                       | <i>vlan-range</i> | Range of the VLANs processing MAC address update packets. |

**Defaults** All VLANs process MAC address update packets.

**Command Mode** Global configuration mode.

**Usage Guide** This command can be used to disable some VLANs from processing MAC address update packets. VLANs disabled from processing MAC address update packets can still recover downlink data transmission of the uplink device using MAC address update packets, but the capability to provide convergence on link failure will be degraded.

**Configuration Examples** The following example configures VLANs processing MAC address update packets:

```
Ruijie(config)# no mac-address-table move update receive vlan 20
```

| Related Commands | Command                                      | Description                                         |
|------------------|----------------------------------------------|-----------------------------------------------------|
|                  | <b>mac-address-table move update receive</b> | Enables REUP to receive MAC address update packets. |

**Platform** N/A.

**Description**

## 1.6 mac-address-table move update transit

Use this command to enable REUP to transmit the mac-address-table update messages.

**mac-address-table move update transit**

**no mac-address-table move update transit**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A.      | N/A.        |

**Defaults** Disabled.

**Command** Global configuration mode.  
**Mode**

**Usage Guide** In order to reduce the link switchover and the loss of the downstream data flow, it is necessary to enable the switch of receiving the MAC address update messages on the uplink switch.

**Configuration Examples** Ruijie(config)# mac-address-table move update transit

**Related Commands**

| Command                                           | Description                                                     |
|---------------------------------------------------|-----------------------------------------------------------------|
| <b>mac-address-table move update transit vlan</b> | Enables REUP to transmit the mac-address-table update messages. |

**Platform** N/A.  
**Description**

## 1.7 mac-address-table move update transit vlan

Use this command to enable REUP to transmit the mac-address update messages.

**mac-address-table move update transit vlan** *vid*

**no mac-address-table move update transit vlan**

**Parameter Description**

| Parameter  | Description                                             |
|------------|---------------------------------------------------------|
| <i>vid</i> | ID of the VLAN transmitting MAC address update packets. |

**Defaults** Transmit the MAC-address update messages in the default VLAN on the port.

**Command Mode** Interface configuration mode.

**Usage Guide** When a link is switched, the VLAN enabled to transmit MAC address update packets will send MAC address update packets to its uplink device.

**Configuration Examples** The following example configures VLANs transmitting MAC address update packets:

**Examples** Ruijie(config)# mac-address-table move update transit

**Related Commands**

| Command                                      | Description                                                    |
|----------------------------------------------|----------------------------------------------------------------|
| <b>mac-address-table move update transit</b> | Enables REUP to receive the mac-address-table update messages. |

**Platform** N/A.

## Description

## 1.8 mac-address-table update group

Use this command to set the mac-address-table update group.

**mac-address-table update group** [ *group-num* ]

**no mac-address-table update group**

| Parameter Description | Parameter        | Description                            |
|-----------------------|------------------|----------------------------------------|
|                       | <i>group-num</i> | The mac-address-table update group ID. |

**Defaults** The default group number is 1.  
By default, no mac-address-table update group is configured.

**Command Mode** Interface configuration mode.

**Usage Guide** In order to reduce the flood due to the MAC address update and the influence on the normal data transmission of the switch, Ruijie products add a configuration of MAC address update group. Only if all the interfaces are added to a MAC address update group, the downstream data transmission be restored rapidly.

**Configuration Examples** Ruijie(config-if)# mac-address-table update group 2

| Related Commands | Command                                           | Description                                              |
|------------------|---------------------------------------------------|----------------------------------------------------------|
|                  | <b>show mac-address-table update group detail</b> | Displays the mac-address-table update group information. |

**Platform Description** N/A.

## 1.9 switchport backup interface *interface-id*

Use this command to configure the REUP dual link backup interface.

**switchport backup interface** *interface-id*

**no switchport backup**

| Parameter Description | Parameter           | Description                      |
|-----------------------|---------------------|----------------------------------|
|                       | <i>interface-id</i> | Interface ID of the backup link. |



**Defaults** N/A.

**Command Mode** Interface configuration mode.

**Usage Guide** Enter the primary interface configuration mode, the interface-id in the parameter is for the backup interface. When the active link fails, the backup link transmission is restored rapidly

**Configuration Examples** The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as primary interface and backup interface:

```
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# switchport backup interface fa 0/2
```

**Related Commands**

| Command                                 | Description                                                |
|-----------------------------------------|------------------------------------------------------------|
| <b>show interface switchport backup</b> | Displays the dual link backup configuration on the switch. |

**Platform Description** N/A.

## 1.10 switchport backup interface preemption

Use this command to configure the REUP link preemption function.

**switchport backup interface** *interface-id* **preemption mode** { **forced** | **bandwidth** | **off** }

**switchport backup interface** *interface-id* **preemption delay** *delay-time*

**no switchport backup interface** *interface-id* **preemption delay**

**Parameter Description**

| Parameter           | Description                          |
|---------------------|--------------------------------------|
| <i>interface-id</i> | The interface id of the backup link. |
| <i>delay-time</i>   | The preemption delay time.           |

**Defaults** The preemption function is disabled by default.  
The default preemption delay time is 35s.

**Command Mode** Interface configuration mode.

**Usage Guide** The preemption mode includes **forced**, **bandwidth** and **off**. In the **bandwidth** preemption mode, the interface with high bandwidth has priority over other interfaces to transmit the data. In the **forced** preemption mode, the primary has priority over backup interfaces to transmit the data. No preemption event occurs in the **off** preemption mode. By default, the preemption mode is off.

The preemption delay refers to the delay time of the link switchover after the restoration of the link failure.

**Configuration Examples** The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as the primary interface and backup interface, set the bandwidth preemption mode and 40s preemption delay:

```
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# switchport backup interface fa 0/2
preemption mode bandwidth
Ruijie(config-if)# switchport backup interface fa 0/2
preemption delay 40
```

**Related Commands**

| Command                                 | Description                                  |
|-----------------------------------------|----------------------------------------------|
| <b>show interface switchport backup</b> | Displays the dual link backup configuration. |

**Platform Description** N/A.

## 1.11 switchport backup interface prefer

Use this command to configure VLAN load balancing on a link. The **no** form of this command is used to delete the configured VLAN load strategy.

**switchport backup interface** *interface-id* **prefer** *instance-range*  
**no switchport backup interface** *interface-id* **prefer**

**Parameter Description**

| Parameter             | Description                                        |
|-----------------------|----------------------------------------------------|
| <i>interface-id</i>   | Interface ID of the backup link.                   |
| <i>instance-range</i> | Instance range of loading on the backup interface. |

**Defaults** No VLAN load on the backup interface.

**Command Mode** Interface configuration mode.

**Usage Guide** MSTP instance mapping can be used to modify the mapping between an instance and a VLAN.

**Configuration Examples** The following example configures VLAN load balancing on dual links.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2 prefer
instance 1
```

**Related Commands**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                                         |                                                               |
|-----------------------------------------|---------------------------------------------------------------|
| <b>show interface switchport backup</b> | Displays the configuration of dual-link backup on the switch. |
| <b>spanning-tree mst configuration</b>  | Configures MSTP instances.                                    |

**Platform** N/A.

**Description**

## 1.12 show interfaces switchport backup

Use this command to display the dual link backup information on the interfaces.

**show interfaces** [ *interface-id* ] **switchport backup** [ **detail** ]

| Parameter          | Parameter           | Description                                                   |
|--------------------|---------------------|---------------------------------------------------------------|
| <b>Description</b> | <i>interface-id</i> | The interface id of the dual link backup.                     |
|                    | <b>detail</b>       | Displays the detailed information about the dual link backup. |

**Defaults** Show the dual link backup information on all interfaces.

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** N/A.

**Configuration** Ruijie # show interfaces switchport backup detail

**Examples**

```
Switch Backup Interface Pairs:
Active Interface Backup Interface State

Gi0/23 Gi0/24 Active Up/Backup Standby
Interface Pair : Gi0/23, Gi0/24
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi0/23(1000 Mbits), Gi0/24(1000 Mbits)
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A.    | N/A.        |

**Platform** N/A.

**Description**

## 1.13 show link state group

Use this command to display the information of a link state track group.

**show link state group** *num*

| Parameter Description | Parameter  | Description                     |
|-----------------------|------------|---------------------------------|
|                       | <i>num</i> | ID of a link state track group. |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** The following example displays the link state track group:

### Examples

```
Ruijie # show link state group
Link State Group:1 Status: Enabled, UP
Upstream Interfaces :Gi0/1(Up)
Downstream Interfaces :Gi0/3(Dwn), Gi0/4(Dwn)
Link State Group:2 Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A.    | N/A.        |

**Platform Description** N/A.

## 1.14 show mac-address-table move update

Use this command to display the statistics about the MAC address updates tranceived on the interface.

**show mac-address-table move update**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** Ruijie#show mac-address-table move update

**Examples** Mac address table move update status:

Transit:disable

Receive:disable

Max-update-rate:150

Receive vlan:1-4094

Pair: Ag1,Ag2

| Members | Status | Transit Count | Transit VLAN | Last Transit Time |
|---------|--------|---------------|--------------|-------------------|
| -----   |        |               |              |                   |
| -----   |        |               |              |                   |

|     |      |   |  |  |
|-----|------|---|--|--|
| Ag1 | Down | 0 |  |  |
|-----|------|---|--|--|

|     |      |   |  |  |
|-----|------|---|--|--|
| Ag2 | Down | 0 |  |  |
|-----|------|---|--|--|

Pair: Ag3,Gi0/6

| Members | Status | Transit Count | Transit VLAN | Last Transit Time |
|---------|--------|---------------|--------------|-------------------|
| -----   |        |               |              |                   |
| -----   |        |               |              |                   |

|     |      |   |  |  |
|-----|------|---|--|--|
| Ag3 | Down | 0 |  |  |
|-----|------|---|--|--|

|       |      |   |  |  |
|-------|------|---|--|--|
| Gi0/6 | Down | 0 |  |  |
|-------|------|---|--|--|

Pair: Gi0/1,Gi0/2

| Members | Status | Transit Count | Transit VLAN | Last Transit Time |
|---------|--------|---------------|--------------|-------------------|
| -----   |        |               |              |                   |
| -----   |        |               |              |                   |

|       |    |   |  |  |
|-------|----|---|--|--|
| Gi0/1 | Up | 0 |  |  |
|-------|----|---|--|--|

|       |         |   |  |  |
|-------|---------|---|--|--|
| Gi0/2 | Standby | 0 |  |  |
|-------|---------|---|--|--|

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A.    | N/A.        |

**Platform Description** N/A.

## 1.15 show mac-address-table update group detail

Use this command to display the mac-address-table update group information.

**show mac-address-table update group detail**

| Parameter Description | Parameter     | Description                                                                 |
|-----------------------|---------------|-----------------------------------------------------------------------------|
|                       | <b>detail</b> | Displays the detailed information about the mac-address-table update group. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** Ruijie # configure terminal

**Examples**

```
Ruijie (config)# mac-address-table move update receive
Ruijie (config)# interface range gigabitEthernet 0/3-4
Ruijie (config-if-range)# mac-address-table update group
Ruijie (config-if-range)# end
Ruijie # show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:7
Group member Receive Count Last Receive Switch-ID Receive Time

GigabitEthernet 0/3 0 0000.0000.0000
GigabitEthernet 0/4 0 0000.0000.0000
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A.    | N/A.        |

**Platform Description** N/A.

## 2 RLDP Commands

### 2.1 rldp detect-interval

Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the **no** form of this command to restore the default value.

**rldp detect-interval** *interval*

**no rldp detect-interval**

| Parameter Description | Parameter       | Description                                     |
|-----------------------|-----------------|-------------------------------------------------|
|                       | <i>interval</i> | Detection interval in the range 2 to 15 seconds |

**Defaults** 3 seconds.

**Command Mode** Global configuration mode.

**Usage Guide** In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.

**Configuration Examples** The following example shows how to set the detection interval as 5s:

```
Ruijie(config)# rldp detect-interval 5
```

| Related Commands | Command                | Description                            |
|------------------|------------------------|----------------------------------------|
|                  | <b>rldp detect-max</b> | Sets the maximum number of detections. |

**Platform Description** N/A.

### 2.2 rldp detect-max

Use this command to set the maximum number of sending detection packets on the port. If the neighboring port does not respond when this detection number is exceeded, the link is considered faulty. Use the **no** form of this command to restore it to the default value.

**rldp detect-max** *num*

**no rldp detect-max**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|            |                                                   |
|------------|---------------------------------------------------|
| <i>num</i> | Maximum number of detections in the range 2 to 10 |
|------------|---------------------------------------------------|

**Defaults** 2.

**Command** Global configuration mode.

**Mode**

**Usage Guide** This command is used together with the detection interval to specify the maximum number of detections.

**Configuration** The following example shows how to set the maximum number of detections as 5:

**Examples** Ruijie(config)# rldp detect-max 5

**Related  
Commands**

| Command                     | Description                  |
|-----------------------------|------------------------------|
| <b>rldp detect-interval</b> | Sets the detection interval. |

**Platform** N/A.

**Description**

## 2.3 rldp enable

Use this command to enable RLDP globally. Use the **no** form of this command to disable the function.

**rldp enable**

**no rldp enable**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A.      | N/A.        |

**Defaults** Disabled.

**Command** Global configuration mode.

**Mode**

**Usage Guide** You can enable RLDP on the interface only when the global RLDP is enabled.

**Configuration** The following example shows how to enable RLDP:

**Examples** Ruijie(config)# rldp enable

**Related  
Commands**

| Command          | Description                            |
|------------------|----------------------------------------|
| <b>rldp port</b> | Enables the RLDP function on the port. |



**Platform** N/A.

**Description**

## 2.4 rldp neighbor-negotiation

Use this command to enable RLDP neighbor negotiation. Use the **no** form or **default** form of this command to restore the default setting.

**rldp neighbor-negotiation**

**no rldp neighbor-negotiation**

**default rldp neighbor-negotiation**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A.      | N/A.        |

**Defaults** RLDP neighbor negotiation is disabled by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** With neighbor negotiation enabled, RLDP unidirectional-/bidirectional-link detection starts only after the neighbor negotiation is successful. (Receiving the Prob message from the neighbor indicates the neighbor negotiation is successful.)

**Configuration** The following example shows how to enable RLDP neighbor negotiation:

**Examples**

```
Ruijie#config
Ruijie(config)#rldp neighbor-negotiation
```

| Related Commands | Command          | Description                            |
|------------------|------------------|----------------------------------------|
|                  | <b>rldp port</b> | Enables the RLDP function on the port. |

**Platform** N/A.

**Description**

## 2.5 rldp port

Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the **no** form of this command to disable the function.

**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }**

**no rldp port { unidirection-detect | bidirection-detect | loop-detect }**

| Parameter Description | Parameter                  | Description                           |
|-----------------------|----------------------------|---------------------------------------|
|                       | <b>unidirection-detect</b> | Sets unidirectional link detection.   |
|                       | <b>bidirection-detect</b>  | Sets bidirectional link detection.    |
|                       | <b>loop-detect</b>         | Sets loop detection type.             |
|                       | <b>warning</b>             | Warns the user.                       |
|                       | <b>shutdown-svi</b>        | Shutowns the SVI the port belongs to. |
|                       | <b>shutdown-port</b>       | Shutowns the port.                    |

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Usage Guide** The RLDP detection on the port takes effect only when the global RLDP is enabled.

**Configuration Examples** The following example shows how to configure RLDP detection on fas 0/1, specify the detection type as loop detection, and troubleshooting method as block.

```
Ruijie(config)# interface fas 0/1
Ruijie(config-if)# rldp port loop-detect block
```

| Related Commands | Command            | Description            |
|------------------|--------------------|------------------------|
|                  | <b>rldp enable</b> | Enables RLDP globally. |

**Platform Description** N/A.

## 2.6 rldp reset

Use this command to make all the ports that have been handled using rldp shutdown or disable to perform RLDP detection again.

**rldp reset**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A.      | N/A.        |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** The example below demonstrates how to use this command:

**Examples** Ruijie# rldp reset

**Related  
Commands**

| Command     | Description            |
|-------------|------------------------|
| rldp enable | Enables RLDP globally. |

**Platform** N/A.

**Description**

## 2.7 show rldp

Use this command to display the RLDP information.

**show rldp [ interface *interface-id* ]**

**Parameter  
Description**

| Parameter           | Description  |
|---------------------|--------------|
| <i>interface-id</i> | Interface ID |

**Defaults** N/A.

**Command  
Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** N/A.

**Examples**

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A.    | N/A.        |

**Platform** N/A.

**Description**

## 3 DLDP Commands

### 3.1 clear dldp

Use this command to clear statistics about the times that DLDP is down or up at a specified monitoring point for renewing statistics.

**clear dldp** [ **interface** *interface-name* [ *ip-address* ] ]

| Parameter   | Parameter             | Description                  |
|-------------|-----------------------|------------------------------|
| Description | <i>interface-name</i> | Name of an Layer 3 interface |
|             | <i>ip-address</i>     | IP address of a peer device  |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** DLDP records statistics about the times that DLDP is down or up. You can use this command to clear statistics about the times that DLDP is down or up at a specified monitoring point and renew statistics. If an L3 interface or a device IP address is specified, statistics about the times that DLDP is down or up on the interface at one or all monitoring points will be cleared. If no L3 interface or IP address is specified, statistics about the times that DLDP is down or up at all monitoring points on all interfaces will be cleared.

**Configuration Examples** The following example clears statistics about the times that DLDP is down or up at all monitoring points on all interfaces.

```
Ruijie#clear dldp
```

The following example clears statistics about the times that DLDP is down or up at all monitoring points on the interface *vlan 1*.

```
Ruijie#clear dldp interface vlan 1
```

The following example clears statistics about the times that DLDP is down or up about the peer device 10.83.132.1 on the interface *vlan 1*.

```
Ruijie# clear dldp interface vlan 1 10.83.132.1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 3.2 dldp

Use this command to configure DLDP detection.

Use the **no** form of this command to disable this function .

**dldp** *ip-address* [ *next-hop-ip* ] [ **mac-address** *mac-addr* ] [ **interval** *tick* | **retry** *retry-num* | **resume** *resume-num* ]

**no dldp** *ip-address*

| Parameter   | Parameter                          | Description                                                                                                                                                                                  |
|-------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <i>ip-address</i>                  | IP address of the peer device to be detected                                                                                                                                                 |
|             | <i>next-hop-ip</i>                 | Next-hop IP address specified when the device to be detected belongs to another different network                                                                                            |
|             | <b>mac-address</b> <i>mac-addr</i> | The bound MAC address. If a next hop exists, its MAC address is configured.                                                                                                                  |
|             | <b>interval</b> <i>tick</i>        | Detection interval. The value range is from 1 to 6,000 in the unit of ticks, where 1 tick is equal to 10 milliseconds. The value must be an integral multiple of five.                       |
|             | <b>retry</b> <i>retry-num</i>      | Number of retry times. The value range is from 1 to 3,600.                                                                                                                                   |
|             | <b>resume</b> <i>resume-num</i>    | Number of recovery times of the link to the peer device to be detected, indicating the number of consecutive packets received before a down link turns up. The value range is from 1 to 200. |

**Defaults** By default, *tick* is 100, indicating that the detection interval is 1 second.  
The values of *retry-num* and *resume-num* are both 3.

**Command Mode** Interface configuration mode

**Usage Guide** You can use this command to enable DLDP detection to quickly detect Ethernet link faults.  
DLDP detection detects multiple IP addresses on Layer 3 ports. If they respond no ICMP packets, they are considered down; if one of them recovers response, they are considered up.

**Configuration Examples** The following example enables DLDP detection for the device 10.83.132.10.

```
Ruijie#config
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 10.83.132.1 255.255.255.0
Ruijie(config-if-VLAN 1)#dldp 10.83.132.10
```

The following example enables DLDP detection for the device 10.83.132.10 in another different network segment.

```
Ruijie#config
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 10.83.132.1 255.255.255.0
Ruijie(config-if-VLAN 1)#dldp 10.83.131.10 10.83.132.2
```

The following example disables DLDP detection for the device 10.83.132.10.

```
Ruijie#config
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#no dldp 10.83.132.10
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description**  
N/A

### 3.3 dldp interval

Use this command to set the DLDP detection interval.

Use the **no** form of this command to restore the default setting.

**dldp interval** *tick*

**no dldp interval**

| Parameter Description | Parameter   | Description                                                                                                               |
|-----------------------|-------------|---------------------------------------------------------------------------------------------------------------------------|
|                       | <i>tick</i> | Detection interval (in ticks), in the range from 5 to 6,000. The value must be a multiple of 5. (1tick = 10 milliseconds) |

**Defaults** The default is 10 ticks (100 ms).

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the DLDP detection interval.  
If a device does not receive the reply packets from the peer device within the specific period (the time of this period is equal to that of the *detection packet retransmission interval* multiplied by the *retry count*), the device takes the L3 port as DOWN (though the physical link is up). Once the device receives the reply packets from the peer device, the device takes the L3 port as UP.

**Configuration Examples** The following example sets the DLDP detection interval to 20 ticks.

```
Ruijie#config
Ruijie(config)#dldp interval 20
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description**  
N/A

### 3.4 dldp passive

Use this command to set DLDP to the passive mode.

Use the **no** form of this command to restore the default setting.

**dldp passive**

**no dldp passive**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** The default is the active mode.

**Command Mode** Interface configuration mode

**Usage Guide** If DLDP is enabled on devices at both ends of a link on a network and ICMP Echo packets are sent to each other for link detection, excessive packets exist between the two devices. If only one device sends ICMP Echo packets to the peer device on which the same detection parameters are configured, the peer device can detect whether the packets arrive in time and whether the link between them is normal. This method saves bandwidth and CPU resources.

You can set DLDP to the active mode for one device to initiate ICMP Echo packets, and set DLDP to the passive mode for the other device to passively receive the packets.

The following example sets DLDP to the passive mode.

**Configuration Examples**

```
Ruijie#config
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 10.83.132.1 255.255.255.0 //Set an IP
address for vlan1.
Ruijie(config-if-VLAN 1)#dldp passive
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

### 3.5 dldp retry

Use this command to set the DLDP retry count.

Use the **no** form of this command to restore the default setting.

**dldp retry *retry-num***

**no dldp retry**

|                               |                                                       |                                           |
|-------------------------------|-------------------------------------------------------|-------------------------------------------|
| <b>Parameter</b>              | <b>Parameter</b>                                      | <b>Description</b>                        |
| <b>Description</b>            | <i>retry-num</i>                                      | Retry count, in the range from 1 to 3,600 |
| <b>Defaults</b>               | The default is 3.                                     |                                           |
| <b>Command Mode</b>           | Global configuration mode                             |                                           |
| <b>Usage Guide</b>            | This command is used to set the DLDP retry count.     |                                           |
| <b>Configuration Examples</b> | The following example sets the DLDP retry count to 4. |                                           |
| <b>Examples</b>               | <pre>Ruijie#config Ruijie(config)#dldp retry 4</pre>  |                                           |
| <b>Related Commands</b>       | <b>Command</b>                                        | <b>Description</b>                        |
|                               | N/A                                                   | N/A                                       |
| <b>Platform Description</b>   | N/A                                                   |                                           |

### 3.6 dldp resume

Use this command to set the DLDP recovery count.

Use the **no** form of this command to restore the default setting.

**dldp resume** *resume-num*

**no dldp resume**

|                               |                                                          |                                                                                                                                                                                                                           |
|-------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameter</b>              | <b>Parameter</b>                                         | <b>Description</b>                                                                                                                                                                                                        |
| <b>Description</b>            | <i>resume-num</i>                                        | Recovery count of the peer device link, in the range from 1 to 200. The parameter indicates the number of DLDP detection packets received consecutively from the peer device before the link status goes from DOWN to UP. |
| <b>Defaults</b>               | The default is 3.                                        |                                                                                                                                                                                                                           |
| <b>Command Mode</b>           | Global configuration mode                                |                                                                                                                                                                                                                           |
| <b>Usage Guide</b>            | This command is used to set the DLDP recovery count.     |                                                                                                                                                                                                                           |
| <b>Configuration Examples</b> | The following example sets the DLDP recovery count to 4. |                                                                                                                                                                                                                           |
| <b>Examples</b>               | <pre>Ruijie#config Ruijie(config)#dldp resume 4</pre>    |                                                                                                                                                                                                                           |



| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

### 3.7 show dldp

Use this command to display DLDP configuration information or statistics at various monitoring points.

**show dldp** [ interface *interface-name* ] [ **statistic** ]

| Parameter Description | Parameter             | Description             |
|-----------------------|-----------------------|-------------------------|
|                       | <i>interface-name</i> | Name of an L3 interface |
|                       | <b>statistic</b>      | Statistics              |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** You can use this command with the keyword **statistics** to display statistics at all monitoring points on all interfaces or a specific Layer 3 interface. If a Layer 3 interface is specified, this command displays DLDP configuration and statistics at all monitoring points on the Layer 3 interface.

**Configuration Examples** The following example displays DLDP configuration information at all monitoring points on all interfaces.

```
Ruijie#show dldp
Interface Type Ip Next-hop Interval Retry Resume State

V12 Passive 192.168.6.3 192.168.2.2 10 5 3 Up
V13 Passive 192.168.7.3 10 5 3 Up
V14 Passive 192.168.3.3 192.168.4.2 10 5 3 Up
```

The following example displays DLDP configuration information at all monitoring points on the Layer 3 interface *vlan 2*.

```
Ruijie#show dldp intface vlan2
Interface Type Ip Next-hop Interval Retry Resume State

V12 Passive 192.168.6.3 192.168.2.2 10 5 3 Up
```

The following example displays DLDP statistics at all monitoring points on all interfaces.

```
Ruijie#show dldp statistic
```

```
Interface Type Ip record-time Up-count Down-count

V12 Passive 192.168.6.3 2h34m5s 10 9
V14 Passive 192.168.3.3 1d2h3m52s 10 9
```

The following example displays DLDP statistics at all monitoring points on the Layer 3 interface *vlan 2*.

```
Ruijie#show dldp statistic interface vlan 2
```

```
Interface Type Ip record-time Up-count Down-count

V12 Passive 192.168.6.3 2h34m5s 10 9
```

| Field       | Description                                                                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| record-time | Time length for recording the number of times that DLDP is up or down. The time is displayed in *y***d**h**m**s format:<br>y: year<br>d: day<br>h: hour<br>m: minute<br>s: second<br>Using the <i>Up-count</i> and <i>Down-count</i> parameters, you can check statistics about the number of times that DLDP is up or down within this time length. |
| Up-count    | Number of times that DLDP is up at the specific monitoring point                                                                                                                                                                                                                                                                                     |
| Down-count  | Number times that DLDP is down at the specific monitoring point                                                                                                                                                                                                                                                                                      |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description**  
N/A

## 4 PCAP Commands

### 4.1 packet capture file

Use this command to specify the name of the file to be saved.

**packet capture file** *filename* [**buffer-size** *buf-size*] [**packet-num** *pkt-num*]

Use this command to clear configurations for file saving and restore the configurations for outputting logs.

**clear packet capture file**

| Parameter Description | Parameter       | Description                                                                                                                                                                                             |
|-----------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>filename</i> | Name of the file to be saved                                                                                                                                                                            |
|                       | <i>buf-size</i> | Buffer size. The buffer size is 2 MB by default if this field is not specified. Packet capture automatically stops when the buffer is full.                                                             |
|                       | <i>pkt-num</i>  | Number of captured packets. Packet capture automatically stops when the number of captured packets reaches the specified value. The packet capture will continue by default unless otherwise specified. |

**Command Mode** Privileged EXEC mode

**Usage Guide** The data of captured packets is saved in the file by default after the file name is set. If no file name is set, the data is directly output on the console as system logs. Only 30 packets can be output by default when no file name is set.

**Configuration Example** #Set the name of the file to be saved to **capture.pcap**, and set the number of captured packets to 100.

```
Ruijie# packet capture file flash:capture.pcap packet-num 100
```

**Verification** Run the **show packet capture status** command to check whether the configuration succeeds.

### 4.2 packet capture point

Use this command to create capture points.

**packet capture point** *capture-point-name* **rule** *rule-name* **location** {**interface** *interface-name* | **vlan** *vlan-id* | **control-plane**} {**in** | **out** | **both**}

Use this command to clear capture points.

**clear packet capture point** *capture-point-name*

| Parameter Description | Parameter                 | Description                                                                             |
|-----------------------|---------------------------|-----------------------------------------------------------------------------------------|
|                       | <i>capture-point-name</i> | Name of a capture point                                                                 |
|                       | <i>rule-name</i>          | Name of matching rule, which is defined by using the <b>packet capture rule</b> command |
|                       | <i>interface-name</i>     | Name of the interface for capturing packets                                             |
|                       | <i>vlan-id</i>            | ID of the VLAN for capturing packet                                                     |
|                       | <b>control-plane</b>      | Packet capture on the control plane                                                     |
|                       | <b>in   out   both</b>    | Packet capture direction: inbound, outbound, or bidirectional.                          |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Users can define multiple capture points (a maximum of 4 capture points are supported currently) at the same location as required, to match different capture rules or packet directions. The capture points can work simultaneously without affecting each other.

**Configuration** #Create a capture point for capturing CPU packets on the Gi0/1 interface.

**Example** Ruijie# packet capture point cap-1 rule tcp location interface gi0/1 both

**Verification** Run the **show packet capture status** command to check whether the configuration succeeds.

### 4.3 packet capture rule

Use this command to define a capture matching rule.

```
packet capture rule rule-name [src-mac smac] [dst-mac dmac] [etype type / ip / arp] [src-ip sip sip-mask] [dst-ip dip dip-mask] [src-ipv6 sip6 sip6-prefix] [dst-ipv6 dip6 dip6-prefix][protocol protocol | tcp | udp] [src-port sport] [dst-port dport]
```

Use this command to clear a capture matching rule.

```
clear packet capture rule rule-name
```

| Parameter Description | Parameter                            | Description             |
|-----------------------|--------------------------------------|-------------------------|
|                       | <i>rule-name</i>                     | Name of a matching rule |
|                       | <i>smac</i>                          | Source MAC address      |
|                       | <i>dmac</i>                          | Destination MAC address |
|                       | <i>type</i> / <b>ip</b> / <b>arp</b> | Layer-2 protocol type   |
|                       | <i>sip</i>                           | Source IP address       |
|                       | <i>sip-mask</i>                      | Source IP mask          |
|                       | <i>dip</i>                           | Destination IP address  |
|                       | <i>dip-mask</i>                      | Destination IP mask     |

|                                           |                          |
|-------------------------------------------|--------------------------|
| <i>sipv6</i>                              | Source IPv6 address      |
| <i>sipv6-prefix</i>                       | Source IPv6 prefix       |
| <i>dipv6</i>                              | Destination IPv6 address |
| <i>dipv6-prefix</i>                       | Destination IPv6 prefix  |
| <i>protocol</i>   <b>tcp</b>   <b>udp</b> | Layer-3 protocol type    |
| <i>sport</i>                              | TCP/UDP source port      |
| <i>dport</i>                              | TCP/UDP destination port |

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide**

1. Users can define multiple rules for packet capture and differentiate them by different names. After a rule is defined, the rule needs to be referenced by the capture point to actually take effect.
2. Before deleting the capture rule, all capture points referencing the rule need to be deleted.

**Configuration** #Define a TCP capture matching rule.

**Example** Ruijie# packet capture rule tcp etype ip protocol tcp

**Verification** Run the **show packet capture status** command to check whether the configuration succeeds.

## 4.4 packet capture start

Use this command to start capturing packets.

**packet capture start**

Use this command to stop capturing packets.

**packet capture stop**

| Parameter Description | Parameter    | Description               |
|-----------------------|--------------|---------------------------|
|                       | <b>start</b> | Starts capturing packets. |
|                       | <b>stop</b>  | Stop capturing packets.   |

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide**

1. If the packet capture stop command is not entered after packet capture starts, the packet capture will automatically stop at the capture point when the number of captured packets reaches the specified number. If the packet capture stop condition is not met, run this command to immediately stop the packet capture.
2. Use the packet capture start command to capture packets at all capture points simultaneously.

**Configuration** #Start capturing packet.

**Example** `Ruijie# packet capture start`

**Verification** Run the **show packet capture status** command to check whether the configuration succeeds.

## 4.5 show packet capture status

Use this command to display the packet capture information.

**show packet capture status**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the packet capture information.

**Configuration Example** N/A

#Display the packet capture information as follows:

```
Ruijie#show packet capture status

Capture rules:
 Capture rules tcp:
 etype: 0x0800
 source MAC: 2222.2222.2222
 destination MAC: 1111.1111.1111
 protocol: 0x6
 source IP: 10.10.10.3
 destination IP: 10.10.10.10
 source port: 5
 destination port: 10

Capture points:
 Capture point controlplane:
 Capture rules: tcp
 location: control-plane
 direction: all
 status: stopped
 packets captured(in): 200
 packets captured(out): 200
```

```
Capture file:
 filename: /tmp/test.pcap
 buffer size: 2(MB)
 packets limit: 500
Ruijie#
```

## Field description:

| Field            | Description                        |
|------------------|------------------------------------|
| Capture rule     | Name of a capture rule             |
| etype            | Layer-2 protocol type              |
| source MAC       | Source MAC address                 |
| destination MAC  | Destination MAC address            |
| protocol         | Layer-3 protocol type              |
| source IP        | Source IP address                  |
| destination IP   | Destination IP address             |
| source port      | Source port                        |
| destination port | Destination port                   |
| Capture point    | Name of a capture point            |
| location         | Location of a capture point        |
| direction        | Packet capture direction           |
| buffer size      | Buffer size                        |
| packets limit    | Quantity limit of captured packets |
| filename         | Name of an output file             |
| status           | Packet capture status              |
| packets captured | Number of captured packets         |

N/A

## 5 VRRP Commands

### 5.1 show vrrp

Use this command to display the VRRP information.

**show** [ **ipv6** ] **vrrp** [ **brief** | *group* ]

| Parameter   | Parameter    | Description                                      |
|-------------|--------------|--------------------------------------------------|
| Description | <b>ipv6</b>  | (Optional) Applies to IPv6 VRRP.                 |
|             | <b>brief</b> | (Optional) Displays the brief of the VRRP group. |
|             | <i>group</i> | Number of the VRRP group to be displayed         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** If no optional parameter is used, the information of all VRRP groups is displayed.

**Configuration Examples** The following example displays the information of all VRRP groups.

```
Ruijie# show vrrp
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
```



```
Master Down interval is 9 sec
Ruijie#
```

The following example displays the brief information of the VRRP group.

```
Ruijie# show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
Gi 0/0 1 100 10.82 - P Backup 192.168.201.213 192.168.201.1
Gi 0/0 2 120 10.59 - P Master 192.168.201.217 192.168.201.2
Ruijie#show ipv6 vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
Gi0/13 1 100 3.60 - P Master FE80::1 FE80::2
```

| Related Commands | Command                                                          | Description                                                              |
|------------------|------------------------------------------------------------------|--------------------------------------------------------------------------|
|                  | <code>vrrp group ip <i>ipaddress</i> [ <b>secondary</b> ]</code> | Enables the VRRP function and set the IP address for the virtual device. |

**Platform** N/A

**Description**

## 5.2 show vrrp interface

Use this command to display the information of the VRRP on the interface.

```
show [ipv6] vrrp interface type number [brief]
```

| Parameter Description | Parameter           | Description                                                       |
|-----------------------|---------------------|-------------------------------------------------------------------|
|                       | <code>ipv6</code>   | (Optional) Applies to IPv6 VRRP.                                  |
|                       | <code>type</code>   | Interface type                                                    |
|                       | <code>number</code> | Interface number                                                  |
|                       | <code>brief</code>  | (Optional) Displays the brief of the VRRP group on the interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the VRRP information on Ethernet interface E1/0.

```
Ruijie# show vrrp interface fastethernet 0/0
FastEthernet 0/0 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
```

```

Preemption is enabled
min delay is 0 sec
Priority is 100
Master Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/0 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec

```

| Related  | Command                                             | Description                                                             |
|----------|-----------------------------------------------------|-------------------------------------------------------------------------|
| Commands | <code>vrrp group ip ip address [ secondary ]</code> | Enables the VRRP function and set the IP address for the virtual device |

**Platform** N/A

**Description**

### 5.3 show vrrp packet statistics

Use this command to display the statistics of the VRRP packet transmission.

**show vrrp packet statistics** [ *interface-type interface-number* ]

| Parameter   | Parameter               | Description               |
|-------------|-------------------------|---------------------------|
| Description | <i>interface-type</i>   | Interface type and number |
|             | <i>interface-number</i> |                           |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistics of VRRP packet transmission on all interfaces.

**Examples** Ruijie# show vrrp packet statistics

```
Total
 InReceives: 966043 packets, InOctets: 38641824, InErrors: 38826
 OutTransmits: 306079, OutOctets: 7798564
GigabitEthernet 3/0/1
 InReceives: 799665 packets, InOctets: 31986600, InErrors: 19657
 OutTransmits: 272931, OutOctets: 6675320
GigabitEthernet 3/0/2
 InReceives: 0 packets, InOctets: 0, InErrors: 0
 OutTransmits: 681, OutOctets: 16344
```

The following example displays the statistics of VRRP packets on the interface gigabitEthernet 3/0/1.

```
Ruijie#show vrrp packet statistics gigabitEthernet 3/0/1
GigabitEthernet 3/0/1
 InReceives: 799911 packets, InOctets: 31996440, InErrors: 19657
 OutTransmits: 273053, OutOctets: 6677760
```

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

**Platform** N/A  
**Description**

## 5.4 vrrp accept\_mode

Use this command to enable the packet accepting function on the IPv6 VRRP virtual router.

Use the **no** form of this command to disable this function.

**vrrp ipv6 group accept\_mode**


**no vrrp ipv6 group accept\_mode**

| Parameter   | Parameter    | Description       |
|-------------|--------------|-------------------|
| Description | <i>group</i> | VRRP group number |

**Defaults** The master IPv6 VRRP is not allowed to accept packets whose destination IPv6 address is the IPv6 address of a virtual router. However, the NA and NS packets should be accepted regardless of the configuration of Accept\_Mode. Also, the master IPv6 VRRP virtual router in the owner state will accept and process any packets whose destination IPv6 address is the IPv6 address of a virtual router, regardless of the configuration of Accept\_Mode.

**Command Mode** Interface configuration mode

**Usage Guide** Configuration of the network interface is effective for the master virtual router.

 Only IPv6 VRRP has this configuration mode.

**Configuration** The following example enables the accept mode on the group 1.

**Examples**

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 accept_mode
```

**Platform** N/A

**Description**

## 5.5 vrrp authentication

Use this command to enable VRRP authentication.

Use the **no** form of this command to disable this function.

**vrrp group authentication string**

**no vrrp group authentication**

| Parameter          | Parameter     | Description                                                                   |
|--------------------|---------------|-------------------------------------------------------------------------------|
| <b>Description</b> | <i>group</i>  | VRRP group number                                                             |
|                    | <i>string</i> | String for the VRRP group authentication (within 8 bytes, plaintext password) |

**Defaults** This function is disabled by default. Even if the VRRP function is enabled, no authentication password is configured by default.

**Command Mode** Interface configuration mode

**Usage Guide** The devices in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration.

**Configuration** The following example sets the authentication password for VRRP group 1.

**Examples**

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
```

```
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 authentication x30dn78k
```

**Platform** N/A

**Description**

## 5.6 vrrp bfd (Global Configuration Mode)

Use this command to enable the global BFD correlation for the IPv4 VRRP backup group to detect the master router status.

Use the **no** form of this command to remove the BFD correlation for IPv4 VRRP.

**vrrp bfd** *interface-type interface-number ip-address*

**no vrrp bfd**

| Parameter          | Parameter               | Description                         |
|--------------------|-------------------------|-------------------------------------|
| <b>Description</b> | <i>interface-type</i>   | Interface type and interface number |
|                    | <i>interface-number</i> |                                     |
|                    | <i>ip-address</i>       | Neighbor IP address                 |

**Defaults** By default, the global BFD correlation for IPv4 VRRP is disabled.

**Command** Global configuration mode

**Mode**

**Usage Guide** After the global BFD correlation for IPv4 VRRP is configured, the BFD correlation configuration for the IPv4 VRRP groups will be removed.

The global BFD correlation for IPv4 VRRP configured later will override the earlier configuration.

The IP address and BFD session of the interface must be configured before configuring the vrrp bfd command.

The global IPv4 VRRP BFD session applies to the IPv4 VRRP router which consists of two devices only.

**Configuration** The following example enables global BFD correlation for IPv4 VRRP.

**Examples**

```
Ruijie#configure terminal
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.201.11 255.255.255.0
Ruijie(config-if-VLAN 1)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if-VLAN 1)#exit
Ruijie(config)# vrrp bfd vlan 1 192.168.201.10
```

| Related         | Command | Description |
|-----------------|---------|-------------|
| <b>Commands</b> | N/A     | N/A         |

**Platform** N/A

**Description**

## 5.7 vrrp bfd (Interface Configuration Mode)

Use this command to enable BFD correlation for the specified IPv4 VRRP group.

Use the **no** form of this command to remove the BFD correlation for the specified IPv4 VRRP group.

**vrrp group bfd ip-address**

**no vrrp group bfd ip-address**

| Parameter          | Parameter         | Description         |
|--------------------|-------------------|---------------------|
| <b>Description</b> | <i>group</i>      | VRRP group ID       |
|                    | <i>ip-address</i> | Neighbor IP address |

**Defaults** By default, no BFD correlation is configured for the IPv4 VRRP group on the interface.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** After the global BFD correlation for IPv4 VRRP is configured, the BFD correlation configuration for the IPv4 VRRP groups will be removed.

The IP address and BFD session of the interface must be configured before configuring the **vrrp bfd** command.

**Configuration** The following example enables BFD correlation for the VRRP group.

**Examples** On Switch 1:

```
Ruijie#configure terminal
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 1.1.1.2 255.255.255.0
Ruijie(config-if-VLAN 1)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if-VLAN 1)#vrrp 1 ip 1.1.1.1
Ruijie(config-if-VLAN 1)#vrrp 1 bfd 1.1.1.3
```

On Switch 2:

```
Ruijie#configure terminal
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 1.1.1.3 255.255.255.0
Ruijie(config-if-VLAN 1)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if-VLAN 1)#vrrp 1 ip 1.1.1.1
Ruijie(config-if-VLAN 1)#vrrp 1 bfd 1.1.1.2
```

| Related         | Command | Description |
|-----------------|---------|-------------|
| <b>Commands</b> | N/A     | N/A         |

**Platform** N/A

**Description**

## 5.8 vrrp delay

Use this command to set the reload latency of the VRRP group on the interface.

Use the **no** form of this command to restore the default setting.

**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }

**no vrrp delay**

| Parameter   | Parameter                           | Description                                                                                                                                                                      |
|-------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <b>minimum</b> <i>min-seconds</i>   | When the interface is up, VRRP group shall be reloaded after at least min-seconds.                                                                                               |
|             | <b>reload</b> <i>reload-seconds</i> | The reload latency of the VRRP group. If the configured <i>min-seconds</i> is more than <i>reload-seconds</i> , the actual reload latency of the VRRP group will be min-seconds. |

**Defaults** This function is disabled by default.

**Command** Interface configuration mode

**Mode**

**Usage Guide** Use this command to set the reload latency of the VRRP group on the interface, when it is required that the VRRP group shall not be reloaded immediately after the system reloads or the interface is up. The reload latency range is 0 to 60 seconds.

**Configuration Examples** The following example sets the VRRP reload latency on E0 to 10 seconds. When E0 is up, VRRP group 1 shall be reloaded in 10 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#vrrp delay minimum 10 reload 10
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 5.9 vrrp description

Use this command to specify a descriptor for the VRRP.

Use the **no** form of this command to restore the default setting.

**vrrp [ ipv6 ] group description text**

**no vrrp [ ipv6 ] group description**

| Parameter   | Parameter    | Description           |
|-------------|--------------|-----------------------|
| Description | <b>ipv6</b>  | Applies to IPv6 VRRP. |
|             | <i>group</i> | VRRP group number     |
|             | <i>text</i>  | VRRP group descriptor |

**Defaults** This function is disabled by default. Even if the VRRP function is enabled, no VRRP group descriptor is configured by default.

**Command** Interface configuration mode

**Mode**

**Usage Guide** This command will set the descriptor for the VRRP group to facilitate the identification of the VRRP group.

**Configuration Examples** The following example labels the VRRP group 1 on Ethernet interface E0 as Building A – Marketing and Administration.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 description "Building A -
Marketing and Administration"
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 fe80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 description "Building B -
Marketing and Administration"
```

| Related Commands | Command                                       | Description                                                             |
|------------------|-----------------------------------------------|-------------------------------------------------------------------------|
|                  | <b>vrrp group ip ip-address [ secondary ]</b> | Enables the VRRP function and set the IP address for the virtual device |

**Platform** N/A

**Description**

## 5.10 vrrp detection-vlan

Use this command to enable IPv4 VRRP packets to be sent to only the first or a specified Sub VLAN in a Super VLAN interface.

Use the **no** form of this command to enable IPv4 VRRP packets to be sent to all the Sub VLANs in a Super VLAN interface.

**vrrp detection-vlan {first-subvlan | subvlan-id}**

**no vrrp detection-vlan**



| Parameter   | Parameter            | Description                                                                      |
|-------------|----------------------|----------------------------------------------------------------------------------|
| Description | <b>first-subvlan</b> | IPv4 VRRP packets are sent to only the first Sub VLAN in a Super VLAN interface. |
|             | <i>subvlan-id</i>    | IPv4 VRRP packets are sent to a specified Sub VLAN in a Super VLAN interface.    |

**Defaults** By default, IPv4 VRRP packets are sent to only the first Sub VLAN in a Super VLAN interface.

**Command Mode** Interface configuration mode

**Usage Guide** Use this command to configure the mode in which IPv4 VRRP packets are sent to a Super VLAN interface. There are three modes in which IPv4 VRRP packets are sent to a Super VLAN interface: to only the first Sub VLAN, to a specified Sub VLAN, or all Sub VLANs.

 This command is configured on a VLAN interface and applies only to Super VLAN interfaces.

**Configuration** The following example enables IPv4 VRRP packets to be sent to all Sub VLANs in Super VLAN 3.

```
Ruijie#configure terminal
Ruijie(config)# vlan 3
Ruijie(config-vlan)# supervlan
Ruijie(config-vlan)# subvlan 5-10
Ruijie(config-vlan)#exit
Ruijie(config)#interface vlan 3
Ruijie(config-if)# no vrrp detection-vlan
```

| Related Commands | Command        | Description                                                   |
|------------------|----------------|---------------------------------------------------------------|
|                  | <b>vrrp ip</b> | Enables the VRRP function and set the IP address of the VRRP. |

**Platform** N/A  
**Description**

## 5.11 vrrp ip

Use this command to enable VRRP on the interface and specify the related virtual IP address.

Use the **no** form of this command to restore the default setting.

**vrrp group ip ipaddress [ secondary ]**

**no vrrp group ip ipaddress [ secondary ]**

| Parameter   | Parameter        | Description                             |
|-------------|------------------|-----------------------------------------|
| Description | <i>group</i>     | VRRP group number of the virtual device |
|             | <i>ipaddress</i> | IP address of the virtual device        |

|                  |                                                           |
|------------------|-----------------------------------------------------------|
| <b>secondary</b> | Specifies the secondary IP address of the virtual device. |
|------------------|-----------------------------------------------------------|

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** If the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual device. Note that if the VRRP group is using the IP address of the Ethernet interface, an error occurs when you remove the IP address of the VRRP group with the **no** command, because there are duplicated IP addresses in the LAN.

**Configuration Examples** The following example enables the VRRP function on Ethernet interface 0. The VRRP group number is 1, primary IP address of the virtual device is 10.0.1.20 and secondary IP address is 10.0.2.20.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.2.1 255.255.255.0
secondary
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.2.20 secondary
```

| Related Commands | Command                            | Description                      |
|------------------|------------------------------------|----------------------------------|
|                  | <b>show vrrp [ brief   group ]</b> | Displays the VRRP configuration. |

**Platform Description** N/A

## 5.12 vrrp ipv6

Use this command to enable IPv6 VRRP on the interface and specify the related virtual IPv6 address. Use the **no** form of the command to restore the default setting.

**vrrp group ipv6 ipv6-address**  
**no vrrp group ip ipv6-address**

| Parameter Description | Parameter           | Description                             |
|-----------------------|---------------------|-----------------------------------------|
|                       | <i>group</i>        | VRRP group number of the virtual device |
|                       | <i>ipv6-address</i> | IPv6 address of the virtual device      |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** IPv6 VRRP and IPv4 VRRP share group numbers ranging from 1 to 255. One VRRP group number of an interface is applicable to both IPv4 VRRP and IPv6 VRRP at the same time. The first configured address should be the link's local address, which cannot be deleted until the other virtual addresses are deleted.

**Configuration Examples** The following example enables the IPv6 VRRP function on Ethernet interface FastEthernet 0/0 with VRRP group number 1 and virtual IPv6 address FE80::1 and 2001::1.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
```

| Related Commands | Command                                 | Description                           |
|------------------|-----------------------------------------|---------------------------------------|
|                  | <b>show ipv6 vrrp [ brief   group ]</b> | Displays the IPv6 VRRP configuration. |

**Platform** N/A  
**Description**

## 5.13 vrrp preempt

Use this command to set the preemption mode of the VRRP group.

Use the **no** form of this command to restore the default setting.

**vrrp [ ipv6 ] group preempt [ delay seconds ]**

**no vrrp [ ipv6 ] group preempt [ delay ]**

| Parameter          | Parameter            | Description                                                                                      |
|--------------------|----------------------|--------------------------------------------------------------------------------------------------|
| <b>Description</b> | <b>ipv6</b>          | Applies to IPv6 VRRP.                                                                            |
|                    | <i>group</i>         | VRRP group number                                                                                |
|                    | <b>delay seconds</b> | (Optional)Specifies the delay before a device declares itself master.<br>The default value is 0. |

**Defaults** This function is disabled by default. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

**Command Mode** Interface configuration mode

**Usage Guide** If the VRRP group is working in the preemption mode, once a device finds its priority is higher than the priority of the master, it will become the master device of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the master's

priority, it will not become the master device of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because that VRRP group has the highest priority and thus automatically becomes the master device in the VRRP group.

**Configuration Examples** The following example enables IPv4 VRRP on interface GigabitEthernet 0/0. When VRRP group 1 finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 preempt delay 15
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 200
```

The following example enables IPv4 VRRP on interface GigabitEthernet 0/0. When VRRP group 1 finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 preempt delay 15
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 200
```

| Related Commands | Command                                                    | Description                                                              |
|------------------|------------------------------------------------------------|--------------------------------------------------------------------------|
|                  | <b>vrrp group ip</b> <i>ipaddress</i> [ <b>secondary</b> ] | Enables the VRRP function and set the IP address for the virtual device. |
|                  | <b>vrrp group priority</b> <i>level</i>                    | Sets the VRRP group priority.                                            |

**Platform** N/A

**Description**

## 5.14 vrrp priority

Use this command to specify the priority of the VRRP group.

Use the **no** form of this command to restore the default setting.

**vrrp** [ **ipv6** ] *group priority level*

**no vrrp** [ **ipv6** ] *group priority*

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |              |                                                |
|--------------------|--------------|------------------------------------------------|
| <b>Description</b> | <b>ipv6</b>  | Specifies the priority of the IPv6 VRRP group. |
|                    | <i>group</i> | VRRP group number                              |
|                    | <i>level</i> | VRRP group priority                            |

**Defaults** This function is disabled by default. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

**Command** Interface configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the priority of IPv4 VRRP group 1 as 254.

**Examples**

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
```

The following example sets the priority of IPv6 VRRP group 1 as 254.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254
```

| <b>Related Commands</b> | <b>Command</b>                                             | <b>Description</b>                                                       |
|-------------------------|------------------------------------------------------------|--------------------------------------------------------------------------|
|                         | <b>vrrp group ip <i>ipaddress</i> [ <b>secondary</b> ]</b> | Enables the VRRP function and set the IP address for the virtual device. |
|                         | <b>vrrp group preempt [ <b>delay seconds</b> ]</b>         | Sets the VRRP in the preemption mode.                                    |

**Platform** N/A

**Description**

## 5.15 vrrp timers advertise

Use this command to specify the interval for the master device to send the VRRP advertisement.

Use the **no** form of this command to restore the default setting.

**vrrp [ **ipv6** ] group **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }**

**no vrrp [ **ipv6** ] group **timers advertise****

| Parameter          | Parameter                               | Description                                                                                                                                                                                                                                |
|--------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <b>ipv6</b>                             | Applies to IPv6 VRRP.                                                                                                                                                                                                                      |
|                    | <i>group</i>                            | VRRP group number                                                                                                                                                                                                                          |
|                    | <i>advertise-interval</i>               | Sets the interval time in seconds between sending VRRP advertisement.                                                                                                                                                                      |
|                    | <b>csec</b> <i>centisecond-interval</i> | Sets the interval time in milliseconds between sending advertisement frames from the master VRRP router in the backup group. The range is from 50 to 99. This value is not set by default.<br>This parameter takes effect only for VRRPv3. |

**Defaults** This function is disabled by default. Once the VRRP function is enabled, the default advertisement interval of the master device is one second.

**Command** Interface configuration mode

**Mode**

**Usage Guide** If the current device becomes the master device in the VRRP group, it will notify its VRRP status, priority and other information by sending the VRRP advertisement in the set interval.  
Based on the RFC specification, the maximum advertisement interval of the IPv4/IPv6 VRRPv3 group is 40 seconds. The advertisement interval can be configured larger than 40 seconds, but the effective advertisement interval is 40 seconds.

**Configuration** The following example sets the IPv4 VRRP advertisement interval as 4 seconds.

**Examples**

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 4
```

The following example sets the IPv6 VRRP advertisement interval as 4 seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise 4
```

The following example sets the IPv4 VRRP advertisement interval as 50 centi-seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
```

```
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise csec 50
```

The following example sets the IPv6 VRRP advertisement interval as 50 centi-seconds.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise csec 50
```

#### Related Commands

| Command                                                          | Description                                                              |
|------------------------------------------------------------------|--------------------------------------------------------------------------|
| <code>vrrp group ip <i>ipaddress</i> [ <b>secondary</b> ]</code> | Enables the VRRP function and set the IP address for the virtual device. |
| <code>vrrp group timers learn</code>                             | Enables the timer learning function.                                     |

**Platform** N/A  
**Description**

## 5.16 vrrp timers learn

Use this command to enable the timer learning function.

Use the **no** form of this command to restore the default setting.

**vrrp [ ipv6 ] group timers learn**

**no vrrp [ ipv6 ] group timers learn**

| Parameter          | Parameter          | Description           |
|--------------------|--------------------|-----------------------|
| <b>Description</b> | <code>ipv6</code>  | Applies to IPv6 VRRP. |
|                    | <code>group</code> | VRRP group number     |

**Defaults** This function is disabled by default. Even if the VRRP function is enabled, the timer learning function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** Once the timer learning function is enabled, if the current device is a VRRP backup device, it will learn the VRRP advertisement interval from the VRRP advertisement of the master device, with which it calculates the master device's failure interval instead of the VRRP advertisement interval configured locally. This command may synchronize the VRRP advertisement timer with the master device.

**Configuration Examples** The following example enables the timer learning function on the IPv4 VRRP group 1.

```
Ruijie#configure terminal
```

```
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers learn
```

The following example to enables the timer learning function on the IPv6 VRRP group 1.

```
vrrp ipv6 1 timers learn
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers learn
```

#### Related Commands

| Command                                                    | Description                                                                |
|------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>vrrp group ip</b> <i>ipaddress</i> [ <b>secondary</b> ] | Enables the VRRP function and set the IP address for the virtual device.   |
| <b>vrrp group ipv6</b> <i>ipaddress</i>                    | Enables the VRRP function and set the IPv6 address for the virtual device. |
| <b>vrrp group timers advertise</b> <i>interval</i>         | Sets the IPv4 VRRP advertising interval.                                   |
| <b>vrrp ipv6 group timers advertise</b> <i>interval</i>    | Sets the IPv6 VRRP advertising interval.                                   |

**Platform** N/A  
**Description**

## 5.17 vrrp track

Use these commands to enable the IPv4/IPv6 VRRP track in the interface configuration mode. Use the **no** form of these commands to restore the default setting.

```
vrrp group track { interface-type interface-number | bfd interface-type interface-number
ipv4-address } [priority]
vrrp ipv6 group track interface-type interface-number [priority]
no vrrp [ipv6] group track interface-type interface-number
```

Use these commands to enable VRRP IPv4/IPv6 address track. Use the **no** form of these commands to restore the default setting.

```
vrrp group track ipv4-address [interval interval-value] [timeout timeout-value] [retry retry-value]
[priority]
vrrp ipv6 group track { ipv6-global-address | ipv6-linklocal-address interface-type interface-number }
[interval interval-value] [timeout timeout-value] [retry retry-value] [priority]
no vrrp group track ipv4-address
```



**no vrrp ipv6 group track** { *ipv6-global-address* | *ipv6-linklocal-address* *interface-type* *interface-number* }

Use this command to disable the specified neighbor IP address track via BFD.





**no vrrp group track bfd** *interface-type* *interface-number* *ipv4-address*

| Parameter                     | Parameter                                                                       | Description                                                                                                                                            |
|-------------------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                   | <i>group</i>                                                                    | VRRP group number                                                                                                                                      |
|                               | <i>interface-type</i><br><i>interface-number</i>                                | Type of monitored interface                                                                                                                            |
|                               | <b>bfd</b> <i>interface-type</i><br><i>interface-number</i> <i>ipv4-address</i> | Enables the specified neighbor IP address track via BFD.                                                                                               |
|                               | <i>priority</i>                                                                 | VRRP priority change range when the interface or ip address reachability status changes. If this parameter is not selected, the default value is 10.   |
|                               | <b>ipv6</b>                                                                     | Applies to IPv6 VRRP.                                                                                                                                  |
|                               | <i>ipv4-address</i>                                                             | Monitored IPv4 address. With BFD configured, it refers to the neighbor IP address.                                                                     |
|                               | <b>interval</b> <i>interval-value</i>                                           | The interval of time to probe whether the monitored ip address is reachable or not. If this parameter is not selected, the default value is 3 seconds. |
|                               | <b>timeout</b> <i>timeout-value</i>                                             | The timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1 seconds.                           |
|                               | <b>retry</b> <i>retry-value</i>                                                 | Track retries. If the value is reached, the link is thought unreachable. If this parameter is not configured, the default value is 3.                  |
|                               | <i>ipv6-global-address</i>                                                      | Global unicast IPv6 address                                                                                                                            |
| <i>ipv6-linklocal-address</i> | Local link IPv6 address                                                         |                                                                                                                                                        |

**Defaults** This function is disabled by default. Even if the VRRP function is enabled, no interface or IP address is specified.

**Command Mode** Interface configuration mode

#### Usage Guide

-  This command can be used to monitor the outlet links. Note that layer-3 routable logical interfaces can be monitored (such as Routed Port, SVI, Loopback and Tunnel).
-  If a host is monitored, specify the IPv4 address for the IPv4 VRRP router or the IPv6 address for the IPv6 VRRP router.
-  If the host IP address is link-local, an interface must be specified.
-  If a VRRP router owns the IP address of the physical interface, the priority is 255. Keep the priority when the monitored IP address or interface is set.

**Configuration Examples** The following example enables the VRRP group 1 to monitor the routed port Fa1/1. If the Fa1/1 link is disconnected, the priority of the VRRP group decreases by 30. When the Fa1/1 link recovers, the priority of VRRP group 1 is restored.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 1/1 30
```

The following example sets the VRRP to track the specified neighbor IP address 192.168.1.3 through BFD:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface FastEthernet 0/1
Ruijie(config-if)#no switchport //used on the switch.
Ruijie(config-if)#ip address 192.168.1.1 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config)#interface FastEthernet 0/2
Ruijie(config-if)#no switchport //used on the switch
Ruijie(config-if)#ip address 192.168.201.17 255.255.255.0
Ruijie(config-if)#vrrp 1 priority 120
Ruijie(config-if)#vrrp 1 ip 192.168.201.1
Ruijie(config-if)#vrrp 1 track bfd FastEthernet 0/1 192.168.1.3 30
Ruijie(config-if)#end
```

| Related Commands | Command                                                    | Description                                                              |
|------------------|------------------------------------------------------------|--------------------------------------------------------------------------|
|                  | <b>vrrp group ip</b> <i>ipaddress</i> [ <b>secondary</b> ] | Enables the VRRP function and set the IP address for the virtual device. |
|                  | <b>vrrp group priority</b> <i>level</i>                    | Sets the VRRP group priority.                                            |

**Platform** N/A

**Description**

## 5.18 vrrp version

Use this command to configure the version of sending the IPv4 VRRP multicast packets.

For the IPv4 VRRP, there are two versions: VRRPv2 and VRRPv3.

Use the **no** form of this command to restore the default setting.

**vrrp group version { 2 | 3 }**

**no vrrp group version**

| Parameter   | Parameter | Description                                  |
|-------------|-----------|----------------------------------------------|
| Description | 2         | Uses the VRRPv2 version to send the packets. |
|             | 3         | Uses the VRRPv3 version to send the packets. |

**Defaults** The default is VRRPv2.

**Command Mode** Interface configuration mode

**Usage Guide** Considering the compatibility of VRRPv2 and VRRPv3 for the IPv4 VRRP, you can choose the version of VRRP packets based on the actual network environment. VRRPv2 is based on RFC3768 and VRRPv3 is based on RFC 5798.

 This command is applicable to IPv4 VRRP only.

**Configuration Examples** The following example configures the version of sending the IPv4 VRRP packets on the interface gi0/0.

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 version 3
```

| Related Commands | Command                                      | Description                                                              |
|------------------|----------------------------------------------|--------------------------------------------------------------------------|
|                  | <b>vrrp group ip ipaddress [ secondary ]</b> | Enables the VRRP function and set the IP address for the virtual device. |
|                  | <b>vrrp group timers advertise interval</b>  | Sets the interval of sending the VRRP advertisement.                     |

**Platform Description** N/A

## 6 VRRP Plus Commands

### 6.1 show vrrp balance

Use this command to display the VRRP Plus brief or details.

**show vrrp balance** [ **brief** | *group* ]

| Parameter Description | Parameter    | Description                                |
|-----------------------|--------------|--------------------------------------------|
|                       | <b>brief</b> | (Optional) Displays the VRRP Plus brief.   |
|                       | <i>group</i> | (Optional) Displays the VRRP Plus details. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** If no optional parameter is used, the details of all VRRP Plus group are displayed.

**Configuration Examples** The following example displays the details of all VRRP Plus groups.

```
Ruijie#show vrrp balance
VLAN 1 - Group 1
 State is BVG
 Virtual IP address is 192.168.1.54
 Hello time 1 sec, hold time 3 sec
 Load balancing: host-dependent
 Redirect time 300 sec, forwarder time-out 14400 sec
 Weighting 90 (configured 100), thresholds: lower 1, upper 100
 Track object 1, state: down, decrement weight: 10
 There are 2 forwarders
 Forwarder 1 (local)
 MAC address:
 0000.5e00.0101
 Owner ID is 00d0.f822.33ab
 Forwarder 2
 MAC address:
 001a.a916.0201
 Owner ID is 00d0.f822.8800
```

The following example shows the brief of the VRRP Plus group.

```
Ruijie# show vrrp balance brief
Interface Grp State Group Addr MAC addr
VLAN 1 1 BVG 192.168.1.1 0000.5e00.0101
```

| Related Commands | Command                                                                      | Description                                                       |
|------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------|
|                  | <b>vrrp group balance</b>                                                    | Enables the VRRP Plus function.                                   |
|                  | <b>vrrp group load-balancing { host-dependent   round-robin   weighted }</b> | Sets the load balancing policy of the VRRP Plus.                  |
|                  | <b>show vrrp balance interface type number [ brief ]</b>                     | Displays the VRRP Plus running status of the specified interface. |

**Platform** N/A

**Description**

## 6.2 show vrrp balance interface

Use this command to display the actions of the VRRP Plus group on the specified interface.

**show vrrp balance interface type number [ brief ]**

| Parameter Description | Parameter                    | Description                                |
|-----------------------|------------------------------|--------------------------------------------|
|                       | <b>interface type number</b> | Specifies the interface type and number.   |
|                       | <b>brief</b>                 | (Optional) Displays the brief information. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the actions of the VRRP Plus on FastEthernet 0/0.

```
Ruijie# show vrrp balance interface FastEthernet 0/0
FastEthernet 0/0 - Group 1
 State is BVG
 Virtual IP address is 192.168.1.54
 Hello time 1 sec, hold time 3 sec
 Load balancing: host-dependent
 Redirect time 300 sec, forwarder time-out 14400 sec
 Weighting 90 (configured 100), thresholds: lower 1, upper 100
 Track object 1, state: down, decrement weight: 10
 There are 2 forwarders
 Forwarder 1 (local)
 MAC address:
 0000.5e00.0101
 Owner ID is 00d0.f822.33ab
```

```
Forwarder 2
MAC address:
 001a.a916.0201
Owner ID is 00d0.f822.8800
```

**Related  
Commands**

| Command                                                                      | Description                                                       |
|------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>vrrp group balance</b>                                                    | Enables the VRRP Plus function.                                   |
| <b>vrrp group load-balancing { host-dependent   round-robin   weighted }</b> | Sets the load balancing policy of the VRRP Plus.                  |
| <b>show vrrp balance interface type number [ brief ]</b>                     | Displays the VRRP Plus running status of the specified interface. |

**Platform** N/A**Description**

## 6.3 vrrp balance

Use this command to enable the VRRP Plus function.

Use the **no** form of this command to disable this function.

**vrrp group balance**

**no vrrp] group balance**

**Parameter  
Description**

| Parameter    | Description                                                       |
|--------------|-------------------------------------------------------------------|
| <i>group</i> | Enables the VRRP Plus function on the VRRP of specified group ID. |

**Defaults** VRRP Plus is disabled by default.**Command  
Mode** Interface configuration mode**Usage Guide** To enable VRRP Plus, you must configure the VRRP group first.**Configuration Examples** The following example enables the VRRP Plus function on the Layer 3 interface GigabitEthernet0/0.

```
Ruijie#config
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.1.1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 balance
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                                    |                                                                   |
|------------------------------------|-------------------------------------------------------------------|
| <b>vrrp load-balancing</b>         | Sets the load balancing policy of the VRRP Plus.                  |
| <b>show vrrp balance</b>           | Displays the VRRP Plus running status.                            |
| <b>show vrrp balance interface</b> | Displays the VRRP Plus running status of the specified interface. |

**Platform** N/A

**Description**

## 6.4 vrrp forwarder preempt

Use this command to enable the forwarding preemption on the VRRP Plus backup group.

Use the **no** form of this command to disable this function.

**vrrp group forwarder preempt**

**no vrrp group forwarder preempt**

**Parameter  
Description**

| Parameter    | Description                                    |
|--------------|------------------------------------------------|
| <i>group</i> | VRRP group number. The range is from 1 to 255. |

**Defaults** By default, forwarding preemption is enabled.

**Command  
Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration  
Examples** The following example enables the forwarding preemption function of the VRRP Plus backup group on the Layer3 interface GigabitEthernet 0/0.

```
Ruijie#config
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.1.1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 balance
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 forwarder preempt
```

**Related  
Commands**

| Command                                                  | Description                                                       |
|----------------------------------------------------------|-------------------------------------------------------------------|
| <b>vrrp group balance</b>                                | Enables the VRRP Plus function.                                   |
| <b>show vrrp balance [ brief   group ]</b>               | Displays the VRRP Plus running status.                            |
| <b>show vrrp balance interface type number [ brief ]</b> | Displays the VRRP Plus running status of the specified interface. |

**Platform** N/A

**Description**

## 6.5 vrrp load-balancing

Use this command to set the VRRP Plus load balancing policy.

Use the **no** form of this command to restore the default setting.

**vrrp group load-balancing** { **host-dependent** | **round-robin** | **weighted**

**no vrrp group load-balancing** { **host-dependent** | **round-robin** | **weighted** }

| Parameter Description | Parameter             | Description                                                                                                                                           |
|-----------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>group</i>          | Specifies the VRRP group ID.                                                                                                                          |
|                       | <b>host-dependent</b> | Sets the host-dependent load balancing policy, so as to use the different virtual MACs to reply the host's ARP request based on different hosts.      |
|                       | <b>round-robin</b>    | Sets the round-robin balancing policy, so as to use the different virtual MACs to reply the host's ARP request in turn, which is the default setting. |
|                       | <b>weighted</b>       | Sets the weight balancing policy, so as to perform the ARP reply based on the device weight of the backup group.                                      |

**Defaults** The default is round-robin.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the load balancing policy of the VRRP Plus group1 on Layer 3 interface GigabitEthernet0/0 as host-dependent.

```
Ruijie# config t
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.1.1
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 balance
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 load-balancing host-dependent
Ruijie(config-if-TenGigabitEthernet 0/2)# vrrp ipv6 1 load-balancing
host-dependent
```

| Related Commands | Command                                                                | Description                                  |
|------------------|------------------------------------------------------------------------|----------------------------------------------|
|                  | <b>vrrp group balance</b>                                              | Enables the VRRP Plus function.              |
|                  | <b>show vrrp balance</b> [ <b>brief</b>   <b>group</b> ]               | Displays the VRRP Plus running status.       |
|                  | <b>show vrrp balance interface</b> <i>type number</i> [ <b>brief</b> ] | Displays the VRRP Plus running status of the |



|  |                      |
|--|----------------------|
|  | specified interface. |
|--|----------------------|

**Platform** N/A

**Description**

## 6.6 vrrp timers redirect

Use this command to set the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group.

Use the **no** form of this command to restore the default value.

**vrrp group timers redirect** *redirect timeout*

**no vrrp group timers redirect**

**Parameter Description**

| Parameter       | Description                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------|
| <i>group</i>    | VRRP Plus backup group ID, in the range of 1 to 255.                                               |
| <i>redirect</i> | The redirection time, 300 seconds (namely 5 minutes) by default, in the range of 0 to 3,600.       |
| <i>timeout</i>  | The timeout, 14,400 seconds (namely 4 hours) by default, in the range of (redirect+600) to 64,800. |

**Defaults** The default redirection interval is 300 seconds and redirection timeout is 14,400 seconds.

**Command** Interface configuration mode

**Mode**

**Usage Guide** The VRRP Plus function should be enabled before setting the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group.

**Configuration Examples** The following example sets the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group.

```
Ruijie#config
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.1.1
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 balance
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 timers redirect 300 6000
```

**Related Commands**

| Command                                    | Description                            |
|--------------------------------------------|----------------------------------------|
| <b>vrrp group balance</b>                  | Enables the VRRP Plus function.        |
| <b>show vrrp balance [ brief   group ]</b> | Displays the VRRP Plus running status. |

|                                                                        |                                                                   |
|------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>show vrrp balance interface</b> <i>type number</i> [ <b>brief</b> ] | Displays the VRRP Plus running status of the specified interface. |
|------------------------------------------------------------------------|-------------------------------------------------------------------|

**Platform** N/A

**Description**

## 6.7 vrrp weighting

Use this command to set the weight and threshold of the VRRP Plus backup group.

Use the **no** form of this command to restore the default setting.

**vrrp group weighting** *maximum* [ **lower** *lower* ] [ **upper** *upper* ]

**no vrrp group weighting**

**Parameter Description**

| Parameter      | Description                                                     |
|----------------|-----------------------------------------------------------------|
| <i>group</i>   | VRRP Plus backup group ID, in the range of 1 to 255.            |
| <i>maximum</i> | Weight, 100 by default, in the range of 2 to 254.               |
| <i>lower</i>   | Weight lower, 1 by default, in the range of 1 to (maximum-1)    |
| <i>upper</i>   | Weight upper, 100 by default, in the range of lower to maximum. |

**Defaults** VRRP Plus backup group weight: 100

Weight lower: 1

Weight upper: 100

**Command Mode** Interface configuration mode

**Mode**

**Usage Guide** The VRRP Plus function should be enabled before setting the weight and threshold of the VRRP Plus backup group

**Configuration Examples** The following example sets the weight and threshold of the VRRP Plus group1.

**Examples**

```
Ruijie#config t
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.1.1
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 balance
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 weighting 50 lower 30 upper 50
```

**Related Commands**

| Command                                                                | Description                                  |
|------------------------------------------------------------------------|----------------------------------------------|
| <b>vrrp group balance</b>                                              | Enables the VRRP Plus function.              |
| <b>show vrrp balance</b> [ <b>brief</b>   <i>group</i> ]               | Displays the VRRP Plus running status.       |
| <b>show vrrp balance interface</b> <i>type number</i> [ <b>brief</b> ] | Displays the VRRP Plus running status of the |

|  |                      |
|--|----------------------|
|  | specified interface. |
|--|----------------------|

**Platform** N/A

**Description**

## 7 BFD Commands

### 7.1 bfd

Use this command to set the BFD session parameters.

Use the **no** form of this command to remove the setting.

**bfd interval** *milliseconds* **min\_rx** *milliseconds* **multiplier** *multiplier-value*

**no bfd interval**

| Parameter Description | Parameter                                 | Description                                                                                                                                        |
|-----------------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>interval</b> <i>milliseconds</i>       | Interval of sending the BFD control messages to the BFD session neighbor.<br><i>milliseconds</i> : The range is from 50 to 10,000 ms.              |
|                       | <b>min_rx</b> <i>milliseconds</i>         | Expected interval of receiving the BFD control messages from the BFD session neighbor.<br><i>milliseconds</i> : The range is from 50 to 10,000 ms. |
|                       | <b>multiplier</b> <i>multiplier-value</i> | Count of BFD control message not received from the peer in the configured interval.<br><i>multiplier-value</i> : The range is from 3 to 50.        |

**Defaults** No BFD session parameter is configured by default.

**Command** Interface configuration mode

**Mode**

**Usage Guide** Those parameters must be configured before enabling the BFD session.  
The express forwarding must be enabled before enabling BFD on the routers.  
BFD session parameters should be consistent on peers, so that associated protocols will take effect at the same time. If not, one-way forwarding will occur.  
Set the parameters based on interface bandwidth. If **interval** and **min\_rx** are too short, BFD sessions may occupy much bandwidth and influence data transmission.

**Configuration** The following example configures the BFD session parameters on routed port FastEthernet 0/2.

**Examples**

```
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config)# no switchport
Ruijie(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 7.2 bfd bind peer-ip

Use this command to create a BFD session to correlate with an interface.

Use the **no** form of this command to remove this setting.

**bfd bind peer-ip** *ip-address* [ **source-ip** *ip-address* ] **process-pst**

**no bfd bind peer-ip** *ip-address*

| Parameter Description | Parameter                          | Description                                                                                                                                                                         |
|-----------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>peer-ip</b> <i>ip-address</i>   | The peer IP address to be detected, which must be directly connected to the Layer 3 interface.                                                                                      |
|                       | <b>source-ip</b> <i>ip-address</i> | Source IP address for sending the BFD packets, which avoids the packets dropped by the URPF in case that this function is used with other functions such the URPF at the same time. |
|                       | <b>process-pst</b>                 | Correlates BFD for the Layer3 interface.                                                                                                                                            |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** Note that this command must be configured a Layer 3 interface and the peer IP address detected must be the address directly-connected to the interface.

**Configuration Examples** The following example detects the peer 1.1.1.2 through BFD on the routed port to generate the BFD status of the interface.

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if -GigabitEthernet 0/2)#no sw
Ruijie(config-if -GigabitEthernet 0/2)#ip address 1.1.1.1 255.255.255.0
Ruijie(config-if -GigabitEthernet 0/2)#bfd bind peer-ip 1.1.1.2 source-ip
1.1.1.1 process-pst
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 7.3 bfd cpp

Use this command to enable the BFD protection policy.

Use the **no** form of this command to disable this function.

**bfd cpp**

**no bfd cpp**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** BFD protocol is so sensitive that if the device with BFD function enabled suffers from attack (for example, a large amount of Ping packets attack the device), which lead to the BFD session turbulence, the device can be protected by enabling the BFD protection policy. However, if the BFD function and the BFD protection policy are enabled at the same time, the loss of BFD packets on the attacked device occurs when the packets sent from the last-hop device go through this device, influencing the BFD session establishment between the last-hop device and other devices. This function is valid only for the switches.

**Configuration Examples** The following example enables the BFD protection policy.

```
Ruijie(config)# bfd cpp
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 7.4 bfd echo

Use this command to enable echo mode.

Use the **no** form of this command to disable echo mode.

**bfd echo**

**no bfd echo**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|     |     |
|-----|-----|
| N/A | N/A |
|-----|-----|

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** This command cannot be configured on the AP ports.

By default, with BFD session parameter configured, the system enables the echo mode automatically. The minimum sending and receiving interval for the echo packets are the values of the configured **interval** *milliseconds* and **min\_rx** *milliseconds*.

This command cannot be configured on the AP port.

Before enabling BFD echo mode, it is necessary to use the **no ip redirects** command to disable the ICMP redirection messages sending on the neighbor device of the BFD session, use the **no ip deny land** to disable the DDOS (Land-based attack prevention) function.

With both ends of the BFD session enabled, the echo mode takes effect.

In the process that the forwarding plane of the peer device returns echo packets transmitted by the local end to the local end, the echo packets may be lost due to congestion of the peer device, causing a session detection failure. In this case, configure Quality of Service (QoS) policies to ensure that echo packets are processed preferentially or disable the echo function.

The echo detection function of BFD does not support multi-hop detection. Ensure that the echo function is disabled when configuring multi-hops.

**Configuration Examples** The following example enables the echo mode on the routed port FastEthernet 0/2:

```
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config)# no switchport
Ruijie(config-if)# bfd echo
```

**Related Commands**

| Command               | Description                           |
|-----------------------|---------------------------------------|
| <b>bfd</b>            | Configures the BFD session parameter. |
| <b>bfd slow-timer</b> | Configures the slow-timer time.       |

**Platform Description** N/A

## 7.5 bfd slow-timer

Use this command to set the slow timer, which is used to send the BFD packets in the BFD asynchronous mode.

Use the **no** form of this command to restore the default setting.

**bfd slow-timer** [ *milliseconds* ]

**no bfd slow-timer**

|                               |                                                                   |                                                                                  |
|-------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                  | <b>Description</b>                                                               |
|                               | <i>milliseconds</i>                                               | BFD slow-timer time. The range is from 1,000 to 30,000. The unit is millisecond. |
| <b>Defaults</b>               | The default slow-timer is 3,000 milliseconds.                     |                                                                                  |
| <b>Command Mode</b>           | Global configuration mode                                         |                                                                                  |
| <b>Usage Guide</b>            | N/A                                                               |                                                                                  |
| <b>Configuration Examples</b> | The following example sets the slow-timer to 14,000 milliseconds. |                                                                                  |
|                               | <pre>Ruijie(config)# bfd slow-timer 14000</pre>                   |                                                                                  |
| <b>Related Commands</b>       | <b>Command</b>                                                    | <b>Description</b>                                                               |
|                               | <b>bfd echo</b>                                                   | Enables the BFD echo function                                                    |
| <b>Platform Description</b>   | N/A                                                               |                                                                                  |

## 7.6 bfd up-dampening

Use this command to set the BFD up-dampening time.

Use the **no** form of this command to restore the default setting.

**bfd up-dampening** [ *milliseconds* ]

**no bfd up-dampening**

|                               |                                                                                                                                  |                                                                                                     |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                                                                                 | <b>Description</b>                                                                                  |
|                               | <i>milliseconds</i>                                                                                                              | (Optional) Sets the BFD up-dampening time. The range is from 0 to 300,000. The unit is millisecond. |
| <b>Defaults</b>               | The default is 0 millisecond, which means that the notification is sent to the related application once the session state is UP. |                                                                                                     |
| <b>Command Mode</b>           | Interface configuration mode                                                                                                     |                                                                                                     |
| <b>Usage Guide</b>            | N/A                                                                                                                              |                                                                                                     |
| <b>Configuration Examples</b> | The following example sets the BFD up-dampening time to 60,000 milliseconds.                                                     |                                                                                                     |
|                               | <pre>Ruijie(config)# bfd up-dampening 60000</pre>                                                                                |                                                                                                     |



| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  |         | <b>bfd</b>  |

**Platform** N/A  
**Description**

## 7.7 show bfd neighbors

Use this command to display the BFD session parameters.

```
show bfd neighbors [vrf vrf-name] [client { ap | bgp | isis | ospf | ospfv3 | rip | vrrp | static-route | vrrp-balance | bgp-lsp | ldp-lsp | static-lsp | backward-lsp-with-ip | pst }] [ipv4 ip-address | ipv6 ip-address] [details]
```

| Parameter Description | Parameter                     | Description                                                                  |
|-----------------------|-------------------------------|------------------------------------------------------------------------------|
|                       | <b>vrf</b> <i>vrf-name</i>    | (Optional) sets the neighbor VRF name.                                       |
|                       | <b>client</b>                 | (Optional) specifies the routing protocol.                                   |
|                       | <b>ap</b>                     | Displays the BFD session configuration for Layer 3 aggregate ports.          |
|                       | <b>bgp</b>                    | Displays the BFD session configuration for BGP.                              |
|                       | <b>isis</b>                   | Displays the BFD session configuration for ISIS.                             |
|                       | <b>ospf</b>                   | Displays the BFD session configuration for OSPF.                             |
|                       | <b>ospfv3</b>                 | Displays the BFD session configuration for OSPFv3.                           |
|                       | <b>rip</b>                    | Displays the BFD session configuration for RIP.                              |
|                       | <b>vrrp</b>                   | Displays the BFD session configuration for VRRP.                             |
|                       | <b>static-route</b>           | Displays the BFD session configuration for the static route.                 |
|                       | <b>pbr</b>                    | Displays the BFD session configuration for PBR.                              |
|                       | <b>vrrp-balance</b>           | Displays the BFD session configuration for the VRPP.                         |
|                       | <b>bgp-lsp</b>                | Displays the BFD session configuration for the BGP-LSP.                      |
|                       | <b>ldp-lsp</b>                | Displays the BFD session configuration for the LDP-LSP.                      |
|                       | <b>backward-lsp-with-ip</b>   | Displays the BFD session configuration for the LSP backward IP co-operation. |
|                       | <b>static-lsp</b>             | Displays the BFD session configuration for the static LSP co-operation.      |
|                       | <b>pst</b>                    | Displays the BFD session configuration and the Layer3 interface status.      |
|                       | <b>ipv4</b> <i>ip-address</i> | (Optional) Displays the session information of the specified IPv4 neighbor.  |
|                       | <b>ipv6</b> <i>ip-address</i> | (Optional) Displays the session information of the specified IPv6 neighbor.  |
|                       | <b>details</b>                | (Optional) Displays the configurations in detail.                            |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** In the information displayed by the **show bfd neighbors** command, the OurAddr field means the source address of the session. The "-" is displayed if the source address is not specified, and it occurs in the BFD session for the LSP backward IP correlation.

**Configuration** The following example displays the BFD session configuration.

**Examples**

```
Ruijie# sh bfd neighbors
IPV4 sessions: 1, UP: 1
IPV6 sessions: 0, UP: 0
OurAddr NeighAddr LD/RD RH Holddown(mult) State Int
192.168.24.2 192.168.24.1 8192/8192 Up 0(3) Up GigabitEthernet 0/1
```

The following example displays the BFD session configuration in detail.

```
Ruijie#sh bfd neighbors
IPV4 sessions: 1, UP: 1
IPV6 sessions: 0, UP: 0
OurAddr NeighAddr LD/RD RH/RS Holddown(mult) State Int
192.168.24.2 192.168.24.1 8192/8192 Up 0(3) Up
GigabitEthernet 0/1
Session state is Up and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 3000000, MinRxInt: 3000000, Multiplier: 3
Received MinRxInt 3000000, Multiplier: 3
Holddown (hits): 9000(0), Hello (hits): 3000(36)
Rx Count: 127, Rx Interval (ms) min/max/avg: 40/999/999
Tx Count: 135, Tx Interval (ms) min/max/avg: 1000/1000/999
Registered protocols: VRRP
Uptime: 0:01:19
Last packet:
Version : 1 - Diagnostic : 0
State bit : Up - Demand bit : 0
Poll bit : 0 - Final bit : 0
Multiplier : 3 - Length : 24
My Discr : 8192 - Your Discr : 8192
Min tx interval : 3000000 - Min rx interval: 3000000
Min Echo interval: 50000
```

The following example displays the BFD session configuration for Layer 3 aggregate ports.

```
Ruijie#show bfd neighbors client ap
IPV4 sessions: 1, UP: 0
IPV6 sessions: 0, UP: 0
OurAddr NeighAddr LD/RD RH/RS Holddown(mult) State Int
```

```
192.168.23.1 192.168.23.2 8192/0 Admin 0(3) Down
GigabitEthernet 0/2 (AP 1)
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A

## 8 IP Event Dampening Commands

### 8.1 dampening

Use this command to enable the IP event dampening function on the interface. Use the **no** or **default** form of this command to disable this function.

**dampening** [ *half-life-period* [ *reuse-threshold* *suppress-threshold* *max-suppress* [ **restart** [ *restart-penalty* ] ] ] ] ]

**no dampening**

**default dampening**

| Parameter Description | Parameter                 | Description                                                                                                                             |
|-----------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>half-life-period</i>   | Configures the half-life period of suppression penalty. The range is from 1 to 30. The unit is seconds. The default value is 5 seconds. |
|                       | <i>reuse-threshold</i>    | Configures the penalty threshold to unsuppress the interface. The range is from 1 to 20,000. The default value is 1,000.                |
|                       | <i>suppress-threshold</i> | Configures the penalty threshold to suppress the interface. The range is from 1 to 20,000. The default value is 2,000.                  |
|                       | <i>max-suppress</i>       | Configures the maximum suppress time. The range is from 1 to 255. The default value is 4 times of the <i>half-life-period</i> .         |
|                       | <b>restart</b>            | Activates the restart penalty.                                                                                                          |
|                       | <i>restart-penalty</i>    | Configures the initial penalty value on the interface. The range is from 1 to 20,000. The default value is 2,000.                       |

**Defaults** IP event dampening is disabled by default.

**Command mode** Interface configuration mode.

**Usage Guide** This function will influence the modules of the directly-connected/host route, static route, dynamic route and VRRP. If one interface meets the configuration condition of this command, which is in the suppression status, the above influenced modules consider the status of this interface as DOWN, so as to delete the corresponding route and not transceive the data packets on this interface.

Re-configuring the dampening command on the interface that has been configured this command makes all dampening information on this interface cleared. However, the interface flapping times will be remained unless use the clear counters command to clear the statistical information of the interface.

Too small max-suppress configured may cause the maximum penalty value obtained from the calculation smaller than the suppression threshold to make this interface will not be suppressed forever. Therefore, it belongs to the erroneous configuration. In this case, the following message will prompt for the configuration error:

% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time  
 Besides, when configuring this command, it will prompt the following message as well if the system memory is not enough to save this configuration:

% No memory, configure dampening fail!

For the interface layer switching of the switches (Layer-3 interface to the Layer-2 interface), for example, if one routed port is switched to the switch port, the **dampening** command configured on this interface will be removed.

**Configuration** The following example configures the IP event dampening function.

**Examples**

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

**Related Commands**

| Command                          | Description                                         |
|----------------------------------|-----------------------------------------------------|
| <b>clear counters</b>            | Clears the interface counters.                      |
| <b>show dampening interface</b>  | Displays the statistics of the dampening interface. |
| <b>show interfaces dampening</b> | Displays details of the dampening interface.        |

**Platform** N/A

**Description**

## 8.2 show dampening interface

Use this command to show the statistics of the dampening interface.

**show dampening interface**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command mode** Privileged EXEC mode/ global configuration mode/ interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the statistics of the dampening interface.

**Examples**

```
Ruijie# show dampening interface
3 interfaces are configured with dampening.
No interface is being suppressed.
```

| Related Commands | Command                          | Description                                               |
|------------------|----------------------------------|-----------------------------------------------------------|
|                  | <b>dampening</b>                 | Enables the IP event dampening function on the interface. |
|                  | <b>clear counters</b>            | Clears the interface counters.                            |
|                  | <b>show interfaces dampening</b> | Displays details of IP event dampening configuration.     |

**Platform** N/A  
**Description**

### 8.3 show interfaces dampening

Use this command to display the details of IP event dampening configuration.

**show interfaces** [ *interface-Id* ] **dampening**

| Parameter Description | Parameter | Description         |
|-----------------------|-----------|---------------------|
|                       |           | <i>interface-id</i> |

**Defaults** N/A

**Command mode** Privileged EXEC mode/ global configuration mode/ interface configuration mode

**Usage Guide** If the interface-id is specified, only the dampening information of this specified interface is displayed.

**Configuration** The following example shows the details of IP event dampening configuration.

```
Examples Ruijie# show interfaces dampening Ethernet1/0
Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart
0 0 FALSE 0 5 1000 2000 20 16000 0
```

| Domain  | Description                                   |
|---------|-----------------------------------------------|
| Flaps   | Interface flapping times.                     |
| Penalty | The current penalty value on the interface.   |
| Supp    | Suppressed or not.                            |
| ReuseTm | Time to unsuppress the interface, in seconds. |
| HalfL   | Half-life period, in seconds.                 |
| ReuseV  | Unsuppressed threshold.                       |
| SuppV   | Start suppression threshold.                  |
| MaxSTm  | Maximum suppression time.                     |
| MaxP    | Maximum penalty value.                        |

|         |                                             |
|---------|---------------------------------------------|
| Restart | The initial penalty value on the interface. |
|---------|---------------------------------------------|

**Related  
Commands**

| Command                         | Description                                     |
|---------------------------------|-------------------------------------------------|
| <b>dampening</b>                | Enables the IP event dampening function.        |
| <b>clear counters</b>           | Clears the interface counters.                  |
| <b>show dampening interface</b> | Displays statistics of the dampening interface. |

**Platform  
Description**

N/A

## 9 VSU Commands

### 9.1 dad relay enable

Use this command to enable the Dual-Active Detection (DAD) relay function.

Use the **no** form of this command to restore the default setting.

**dad relay enable**

**no dad relay enable**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** This command is only supported on the aggregate port (AP).

**Configuration Examples** The following example enables the AP-based DAD relay function.

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#dad relay enable
```

The following example disables the AP-based DAD relay function.

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#no dad relay enable
Ruijie(config-if-AggregatePort 1)#exit
```

| Related Commands | Command                                | Description                                                                         |
|------------------|----------------------------------------|-------------------------------------------------------------------------------------|
|                  | <b>dual-active detection</b>           | Configures DAD.                                                                     |
|                  | <b>dual-active pair interface</b>      | Configures a pair of Bidirectional Forwarding Detection (BFD)-based DAD interfaces. |
|                  | <b>dual-active exclude interface</b>   | Configures an exclude interface of DAD.                                             |
|                  | <b>show switch virtual dual-active</b> | Displays the configuration and status of DAD.                                       |

**Platform Description** N/A

### 9.2 dual-active bfd interface

Use this command to configure a BFD port.



Use the **no** form of this command to remove the setting.

**dual-active bfd interface** *interface-name*

**no dual-active bfd interface** *interface-name*

| Parameter   | Parameter             | Description    |
|-------------|-----------------------|----------------|
| Description | <i>interface-name</i> | Interface name |

**Defaults** N/A

**Command Mode** config-vs-domain configuration mode

**Usage Guide** The BFD port must be a routing port on the peer end.

**Configuration** The following examples configures interface Gi 1/1/1 as a BFD port.

**Examples**

```
Ruijie(config)# interface GigabitEthernet 1/1/1
Ruijie(config-if- GigabitEthernet 1/1/1)# no switchport
Ruijie(config)# interface GigabitEthernet 2/1/1
Ruijie(config-if- GigabitEthernet 2/1/1)# no switchport
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/1/1
Ruijie(config-vs-domain)# dual-active bfd interface GigabitEthernet 2/1/1
```

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

**Platform** N/A

**Description**

## 9.3 dual-active detection

Use this command to enable DAD.

Use the **no** form of this command to restore the default setting.

**dual-active detection { bfd | aggregateport }**

**no dual-active detection { bfd | aggregateport }**

| Parameter   | Parameter            | Description   |
|-------------|----------------------|---------------|
| Description | <b>bfd</b>           | BFD-based DAD |
|             | <b>aggregateport</b> | AP-based DAD  |

**Defaults** This function is disabled by default.

**Command Mode** config-vs-domain configuration mode

**Usage Guide** Configure this command only in virtual switch unit (VSU) mode.

**Configuration** The following example enables BFD-based DAD.

**Examples**

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active detection bfd
```

The following example disables BFD-based DAD.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# no dual-active detection bfd
```

The following example enables AP-based DAD.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active detection aggregateport
```

The following example disables AP-based DAD.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)#no dual-active detection aggregateport
```

**Related**

**Commands**

| Command                                | Description                                   |
|----------------------------------------|-----------------------------------------------|
| <b>dual-active pair interface</b>      | Configures a DAD interface.                   |
| <b>dual-active exclude interface</b>   | Configures an exclude interface of DAD.       |
| <b>show switch virtual dual-active</b> | Displays the configuration and status of DAD. |

**Platform**

N/A

**Description**

## 9.4 dual-active exclude interface

Use this command to configure an exclude interface of DAD.

Use the **no** form of this command to remove the exclude interface setting.

**dual-active exclude interface** *interface-name*

**no dual-active exclude interface** *interface-name*

**Parameter**

**Description**

| Parameter             | Description    |
|-----------------------|----------------|
| <i>interface-name</i> | Interface name |

**Defaults**

N/A

**Command Mode**

config-vs-domain configuration mode

**Usage Guide**

Configure this command only in VSU mode.

An exclude interface must be a routing interface instead of a virtual switch link (VSL) interface.

Multiple exclude interfaces are supported.

**Configuration** The following example configures interface Gi 1/1/3 as an exclude interface of DAD.

**Examples**

```
Ruijie(config)# interface GigabitEthernet 1/0/3
Ruijie(config-if-GigabitEthernet 1/0/3)# no switchport
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active exclude interface GigabitEthernet
1/0/3
```

**Related****Commands**

| Command                                | Description                                   |
|----------------------------------------|-----------------------------------------------|
| <b>dual-active detection</b>           | Configures DAD.                               |
| <b>dual-active pair interface</b>      | Configures a DAD interface.                   |
| <b>show switch virtual dual-active</b> | Displays the configuration and status of DAD. |

**Platform**

N/A

**Description**

## 9.5 dual-active interface

Use this command to configure an AP-based DAD interface.

Use the **no** form of this command to remove the setting.

**dual-active interface** *interface-name*

**no dual-active interface**

**Parameter****Description**

| Parameter             | Description                                                                       |
|-----------------------|-----------------------------------------------------------------------------------|
| <i>interface-name</i> | Interface type and interface number. An AP-based DAD interface must be specified. |

**Defaults**

N/A

**Command Mode**

config-vs-domain configuration mode

**Usage Guide**

Only one AP-based detection interface can be configured. Create an AP-based interface before setting it to a detection interface. The previous detection interface will be overwritten by the current detection interface.

**Configuration**

The following example configures AP 1 as the AP-based detection interface.

**Examples**

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#exit
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active interface aggregateport 1
```

**Related****Commands**

| Command                                | Description                                   |
|----------------------------------------|-----------------------------------------------|
| <b>dual-active detection</b>           | Configures BFD-/AP-based DAD.                 |
| <b>show switch virtual dual-active</b> | Displays the configuration and status of DAD. |

**Platform** N/A  
**Description**

## 9.6 port-member interface

Use this command to add a VSL-AP member interface.

Use the **no** form of this command to delete a VSL-AP member interface.

**port-member interface** *interface-name* [ **copper** | **fiber** ]

**no port-member interface** *interface-name*

| Parameter          | Parameter             | Description                                                               |
|--------------------|-----------------------|---------------------------------------------------------------------------|
| <b>Description</b> | <i>interface-name</i> | Interface name, for example, GigabitEthernet 0/1 and GigabitEthernet 0/3. |
|                    | <b>copper</b>         | Copper port                                                               |
|                    | <b>fiber</b>          | Fiber port                                                                |

**Defaults** N/A

**Command Mode** config-vsl-port configuration mode

**Usage Guide** Configure this command in VSU mode or in standalone mode.

**Configuration Examples** The following example adds and deletes a VSL-AP member port in standalone mode.

```
Ruijie(config)# vsl-port
Ruijie(config-vsl-port)# port-member interface GigabitEthernet 0/1
Ruijie(config-vsl-port)# no port-member interface GigabitEthernet 0/2
```

The following example adds and deletes a VSL-AP member port in VSU mode.

```
Ruijie(config)# vsl-port
Ruijie(config-vsl-port)# port-member interface GigabitEthernet 1/1/1
Ruijie(config-vsl-port)# no port-member interface GigabitEthernet 1/1/1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 9.7 show switch id

Use this command to display the device ID.

**show switch id**

|                               |                                                                      |                                                                    |
|-------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>Parameter</b>              | <b>Parameter</b>                                                     | <b>Description</b>                                                 |
| <b>Description</b>            | N/A                                                                  | N/A                                                                |
| <b>Defaults</b>               | N/A                                                                  |                                                                    |
| <b>Command Mode</b>           | Privileged EXEC mode                                                 |                                                                    |
| <b>Usage Guide</b>            | N/A                                                                  |                                                                    |
| <b>Configuration Examples</b> | The following example displays the device ID in the standalone mode. |                                                                    |
|                               | <pre>Ruijie#show switch id Switch ID is 2</pre>                      |                                                                    |
|                               | The following example displays the device ID in the VSU device.      |                                                                    |
|                               | <pre>Ruijie#show switch id Switch ID is 1</pre>                      |                                                                    |
| <b>Related Commands</b>       | <b>Command</b>                                                       | <b>Description</b>                                                 |
|                               | <b>show switch virtual</b>                                           | Displays the domain ID as well as the ID and role of each chassis. |
| <b>Platform Description</b>   | N/A                                                                  |                                                                    |

## 9.8 show switch virtual

Use this command to display the domain ID as well as the ID, status and role of the device.

**show switch virtual**

|                               |                                                                                                                   |                    |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Parameter</b>              | <b>Parameter</b>                                                                                                  | <b>Description</b> |
| <b>Description</b>            | N/A                                                                                                               | N/A                |
| <b>Defaults</b>               | N/A                                                                                                               |                    |
| <b>Command Mode</b>           | Privileged EXEC mode                                                                                              |                    |
| <b>Usage Guide</b>            | N/A                                                                                                               |                    |
| <b>Configuration Examples</b> | The following example displays the domain ID as well as the ID, status and role of the device in standalone mode. |                    |
|                               | <pre>Ruijie# show switch virtual Current system is running in "STANDALONE" mode.</pre>                            |                    |

The following example displays the domain ID as well as the ID, status and role of each device in VSU mode.

```
Ruijie#show switch virtual
Switch_id Domain_id Priority Status Role Description

--
1(1) 1(1) 100(100) OK ACTIVE switch-1
2(2) 1(1) 100(100) OK CANDIDATE switch-2
3(3) 1(1) 100(100) OK STANDBY switch-3
```

**Related  
Commands**

| Command                      | Description                                            |
|------------------------------|--------------------------------------------------------|
| <b>switch</b>                | Modifies the device ID in standalone mode.             |
| <b>switch priority</b>       | Configures the device priority.                        |
| <b>switch renumber</b>       | Modifies the device ID in VSU mode.                    |
| <b>switch domain</b>         | Modifies the domain ID of a device in VSU mode.        |
| <b>switch virtual domain</b> | Modifies the domain ID of a device in standalone mode. |

**Platform  
Description**

N/A

## 9.9 show switch virtual balance

Use this command to display the load balance configuration in VSU mode.

**show switch virtual balance**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

N/A

**Command Mode**

Privileged EXEC mode

**Usage Guide**

N/A

**Configuration**

The following example displays the load balance configuration of the device in VSU mode.

**Examples**

```
Ruijie#show switch virtual balance
Aggregate port LFF: enable
```

**Related  
Commands**

| Command                    | Description                                                      |
|----------------------------|------------------------------------------------------------------|
| <b>show switch virtual</b> | Displays the domain ID as well as the ID and role of the device. |

**Platform**

N/A

Description

## 9.10 show switch virtual config

Use this command to display the VSU configuration of the device in standalone or VSU mode.

**show switch virtual config** [ *switch\_id* ]

| Parameter   | Parameter        | Description                                             |
|-------------|------------------|---------------------------------------------------------|
| Description | <i>switch_id</i> | Displays the VSU configuration of the specified device. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the VSU configuration of the device in standalone mode.

### Examples

```
Ruijie#show switch virtual config
mac: 00d0.f810.3323
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
!
vsl-port
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
switch convert mode standalone
!
```

The following example displays the VSU configuration of the device in VSU mode.

```
Ruijie#show switch virtual config
switch id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
switch 1 description switch1
!
vsl-port
```

```

port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

switch_id: 2 (mac: 00d0.f810.2222)
!
switch virtual domain 1
!
switch 2
switch 2 priority 100
!
vsl-port
port-member interface GigabitEthernet Ethernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
```

The following example displays the VSU configuration of the device 1 in VSU mode.

```

Ruijie#show switch virtual config 1
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
switch 1 description switch1
!
vsl-port
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
```

**Related  
Commands**

| Command                    | Description                                                        |
|----------------------------|--------------------------------------------------------------------|
| <b>show switch virtual</b> | Displays the domain ID as well as the ID and role of each chassis. |

**Platform  
Description**

N/A

## 9.11 show switch virtual dual-active

Use this command to display the configuration of DAD.



**show switch virtual dual-active { bfd | aggregateport | summary }**

| Parameter   | Parameter            | Description                     |
|-------------|----------------------|---------------------------------|
| Description | <b>bfd</b>           | Configuration of BFD-based DAD  |
|             | <b>aggregateport</b> | Configuration of AP-based DAD   |
|             | <b>summary</b>       | Configuration and status of DAD |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration and status of DAD.

**Examples**

```
Ruijie# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: No
Interfaces excluded from shutdown in recovery mode:
GigabitEthernet 1/0/3
GigabitEthernet 1/0/4
In dual-active recovery mode: No
```

The following example displays the configuration of BFD-based DAD.

```
Ruijie# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
 GigabitEthernet 1/0/1: UP
 GigabitEthernet 2/0/2: UP
```

The following example displays the status of AP-based DAD.

```
Ruijie# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
AggregatePort 1: UP
 GigabitEthernet 1/0/1: UP
 GigabitEthernet 2/0/1: UP
 GigabitEthernet 1/0/2: UP
 GigabitEthernet 2/0/2: UP
DAD relay enable AP list:
 AggregatePort 1
```

**Related  
Commands**

| Command                           | Description                 |
|-----------------------------------|-----------------------------|
| <b>dual-active detection</b>      | Enables DAD.                |
| <b>dual-active pair interface</b> | Configures a DAD interface. |

|                                      |                                  |
|--------------------------------------|----------------------------------|
| <b>dual-active exclude interface</b> | Configures an exclude interface. |
|--------------------------------------|----------------------------------|

|                    |     |
|--------------------|-----|
| <b>Platform</b>    | N/A |
| <b>Description</b> |     |

## 9.12 show switch virtual link

Use this command to display the status of a virtual switch link (VSL).

**show switch virtual link [ port ]**

| Parameter          | Parameter   | Description                        |
|--------------------|-------------|------------------------------------|
| <b>Description</b> | <b>port</b> | Displays the port status of a VSL. |

|                 |     |
|-----------------|-----|
| <b>Defaults</b> | N/A |
|-----------------|-----|

|                     |                      |
|---------------------|----------------------|
| <b>Command Mode</b> | Privileged EXEC mode |
|---------------------|----------------------|

|                    |     |
|--------------------|-----|
| <b>Usage Guide</b> | N/A |
|--------------------|-----|

**Configuration** The following example displays VSL link information.

### Examples

```
Ruijie# show switch virtual link
VSL-AP State Peer-VSL Rx Tx Uptime

1/1 UP 2/1 100000 100000 1d,4h,29m
2/1 UP 1/1 100000 100000 1d,4h,29m
```

The following example displays VSL port information.

```
Ruijie# show switch virtual link port

switch 1:
Port AP State Peer-port Rx Tx
 Uptime

GigabitEthernet 1/0/1 1 OK GigabitEthernet 2/0/1 9000 9000
 0d,0h,20m
GigabitEthernet 1/0/2 2 OK GigabitEthernet 2/0/2 9000 9000
 0d,0h,20m

Switch 2:
Port AP State Peer-port Rx Tx
 Uptime

```

```

GigabitEthernet 2/0/1 1 OK GigabitEthernet 1/0/1 9000 9000
 0d, 0h, 20m
GigabitEthernet 2/0/2 2 OK GigabitEthernet 1/0/2 9000 9000
 0d, 0h, 20m

```

**Related  
Commands**

| Command                         | Description                                         |
|---------------------------------|-----------------------------------------------------|
| <b>show switch virtual</b>      | Displays information about the VSU system.          |
| <b>show switch virtual role</b> | Displays the ID, role, and priority of each device. |

**Platform  
Description**

N/A

## 9.13 show switch virtual role

Use this command to display the ID, role, and priority of each chassis.

**show switch virtual role**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

N/A

**Command Mode**

Privileged EXEC mode

**Usage Guide**

N/A

**Configuration  
Examples**

The following example displays the domain ID as well as the ID, status and role of the device in standalone mode.

```

Ruijie# show switch virtual
Current system is running in "STANDALONE" mode.

```

The following example displays the domain ID as well as the ID, status and role of each device in VSU mode.

```

Ruijie#show switch virtual
Switch_id Domain_id Priority Status Role Description

--
1 (1) 1 (1) 100 (100) OK ACTIVE switch-1
2 (2) 1 (1) 100 (100) OK CANDIDATE switch-2
3 (3) 1 (1) 100 (100) OK STANDBY switch-3

```

**Related  
Commands**

| Command                      | Description                                            |
|------------------------------|--------------------------------------------------------|
| <b>switch priority</b>       | Configures the priority of a device in the VSU system. |
| <b>switch virtual domain</b> | Modifies the domain ID of a device in standalone mode. |

|                                 |                           |
|---------------------------------|---------------------------|
| <b>show switch virtual link</b> | Displays VSL information. |
|---------------------------------|---------------------------|

**Platform**  
**Description**

N/A

## 9.14 show switch virtual topology

Use this command to display the VSU topology connection status.

**show switch virtual topology**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults**

N/A

**Command Mode**

Privileged EXEC mode

**Usage Guide**

N/A

**Configuration** The following example displays the topology status.

**Examples**

```
Ruijie# show switch virtual topology
Introduction: '[num]' means switch num, '(num/num)' means vsl-aggregateport
num.

Chain Topology:
[1] (1/2) --- (2/1) [2]

Switch[1]: ACTIVE, MAC: 00d0.f822.33d6, Description: Switch1
Switch[2]: STANDBY, MAC: 1234.5678.9003, Description: Switch2
```

Field Description

| Field         | Description         |
|---------------|---------------------|
| Ring Topology | Topology type.      |
| Switch[-]     | Device description. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform**  
**Description**

N/A


## 9.15 switch

Use this command to specify the ID of a device in the VSU system.

Use the **no** form of this command to restore the default setting.

**switch** *switch\_id*

**no switch**

| Parameter   | Parameter        | Description                                                                                                      |
|-------------|------------------|------------------------------------------------------------------------------------------------------------------|
| Description | <i>switch_id</i> | ID of a device in the VSU system                                                                                 |
|             |                  |  The range depends on products. |

**Defaults** The default is 1.

**Command Mode** config-vs-domain configuration mode

**Usage Guide** The device ID identifies each virtual device member. In VSU mode, the interface name format changes to "switch/slot/port" from "slot/port", in which "switch" is the device ID. If either chassis are active or if the role of the just started chassis is uncertain and both have the same priority, the chassis with a smaller ID is elected as the active one. This command can be only used to modify the device ID in standalone mode. In VSU mode, run the **switch renumber** command to modify the device ID. The modified device ID takes effect only after you restart the device, regardless of in standalone mode or in VSU mode.

**Configuration Examples** The following example sets the ID of the device whose domain ID is 1 to 2 in the VSU system.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 2
Ruijie(config-vs-domain)# exit
```

| Related Commands | Command                      | Description                                                        |
|------------------|------------------------------|--------------------------------------------------------------------|
|                  | <b>switch virtual domain</b> | Modifies the domain ID of a device in standalone mode.             |
|                  | <b>switch priority</b>       | Configures the priority of a device in the VSU system.             |
|                  | <b>show switch virtual</b>   | Displays the domain ID as well as the ID and role of each chassis. |

**Platform** N/A

**Description**

## 9.16 switch convert mode

Use this command to perform conversion between the standalone mode and the VSU mode.

**switch convert mode** { **virtual** | **standalone** } [ *switch\_id* ]

| Parameter   | Parameter         | Description     |
|-------------|-------------------|-----------------|
| Description | <b>virtual</b>    | VSU mode        |
|             | <b>standalone</b> | Standalone mode |
|             | <i>switch_id</i>  | Device ID       |

- Defaults** The device is in standalone mode by default.
- Command Mode** Privileged EXEC mode
- Usage Guide** After you run the **switch convert mode virtual** command, the software automatically backs up the configuration file in standalone mode, saves it as a **standalone.text** file, and then deletes the **config.text** file. The software also prompts you whether to use the **virtual\_switch.text** file to overwrite the **config.text** file, write the VSU-related configurations to the **config\_vsu\_dat** file, and then restart the device.
- After you run the **switch convert mode standalone** command, the active chassis automatically backs up the configuration file in VSU mode, saves it as a **virtual\_switch.text** file, and then deletes the **config.text** file. The active chassis also prompts you whether to use the **standalone.text** file to overwrite the **config.text** file and restart the device.
- The **switch convert mode** command can be used in standalone mode or in VSU mode. In standalone mode, this command is used to switch the mode of the current chassis. In VSU mode, this command is used to switch the mode of the device specified by **switch\_id** if **switch\_id** is available and to switch the mode of the active device if **switch\_id** is not available. You are advised to first switch the mode of the standby device and then the mode of the active mode.

**Configuration** The following example converts the device mode from the standalone mode into the VSU mode.

**Examples** Ruijie# switch convert mode virtual

The following example switches the modes of the standby device (**switch\_id** set to **2**) and the active device (**switch\_id** set to **1**) from the VSU mode to the standalone mode.

```
Ruijie# switch convert mode standalone 2
Ruijie# switch convert mode standalone 1
```

| Related Commands | Command                      | Description                                                       |
|------------------|------------------------------|-------------------------------------------------------------------|
|                  | <b>switch</b>                | Modify the device ID in standalone mode.                          |
|                  | <b>switch virtual domain</b> | Modify the domain ID of a device in standalone mode.              |
|                  | <b>switch priority</b>       | Configure the priority of a device in the VSU system.             |
|                  | <b>show switch virtual</b>   | Display the domain ID as well as the ID and role of each chassis. |

**Platform** N/A  
**Description**

## 9.17 switch crc

Use this command to configure parameters for frame error detection.

Use the **no** form of this command to restore the default setting.

**switch crc errors** *error\_num* **times** *time\_num*

**no switch crc**

| Parameter   | Parameter        | Description                                                                                                                                                       |
|-------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <i>error_num</i> | Limits the number of error frames increasing from that in the last detection. If the increased number is greater than <i>error_num</i> , it is taken as an error. |
|             | <i>time_num</i>  | When the error count exceeds the <i>time_num</i> , the device will take actions (prompting a message or disabling the port).                                      |

**Defaults** The default *error\_num* is 3.  
The default *time\_num* is 10.

**Command Mode** config-vs-domain configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the *error\_time* and *time\_num* parameters to 10 and 5 respectively.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)#
Ruijie(config-vs-domain)#switch crc errors 10 times 5
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 9.18 switch description

Use this command to configure the description for a VSU switch.

Use the **no** form of this command to remove the setting.

**switch** *switch\_id* **description** *dev-name*

**no switch** *switch\_id* **description**

| Parameter   | Parameter        | Description                                        |
|-------------|------------------|----------------------------------------------------|
| Description | <i>switch_id</i> | Device ID                                          |
|             | <i>dev_name</i>  | Device description, no greater than 32 characters. |

**Defaults** N/A

**Command Mode** config-vs-domain configuration mode

**Usage Guide** This command is configured on a device in whether standalone or VSU mode and takes effect immediately after configuration,

**Configuration** The following example configures the description for a VSU switch.

**Examples**

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 description buildingA
Ruijie(config-vs-domain)# exit
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform**  
**Description** N/A


## 9.19 switch domain

Use this command to modify the domain ID of a device in VSU mode.

Use the **no** form of this command to restore the default setting.

**switch** *switch\_id* **domain** *new\_domain\_id*

**no switch** *switch\_id* **domain**

| Parameter Description | Parameter            | Description                                                                                                                                                                                                       |
|-----------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>switch_id</i>     | ID of the running device in VSU mode.<br><br> The range depends on products. For details, see the <i>Configuration Guide</i> . |
|                       | <i>new_domain_id</i> | New domain ID, in the range from 1 to 255.                                                                                                                                                                        |

**Defaults** The default *new\_domain\_id* is 100 by default.

**Command Mode** config-vs-domain configuration mode

**Usage Guide** Use this command only in VSU mode. In addition, the setting can take effect only after the device is restarted.

**Configuration** The following example sets the domain ID of device 1 to 10 in VSU mode.

**Examples**

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 domain 10
```

The following example sets the domain ID of device 2 to 10 in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 2 domain 10
```

The following example sets the domain ID of device 2 to the default value in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# no switch 2 domain
```



| <b>Related<br/>Commands</b> | Command                      | Description                                                        |
|-----------------------------|------------------------------|--------------------------------------------------------------------|
|                             | <b>switch virtual domain</b> | Modifies the domain ID in standalone mode.                         |
|                             | <b>show switch virtual</b>   | Displays the domain ID as well as the ID and role of each chassis. |

**Platform**  
**Description**

N/A


## 9.20 switch priority

Use this command to configure the priority of a device in the VSU system.

Use the **no** form of this command to restore the default setting.

**switch** *switch\_id* **priority** *priority\_num*

**no switch** *switch\_id* **priority**

| <b>Parameter<br/>Description</b> | Parameter           | Description                                                                                                                                                                                                 |
|----------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | <i>switch_id</i>    | ID of a device in the VSU system.<br><br> The range depends on products. For details, see the <i>Configuration Guide</i> . |
|                                  | <i>priority_num</i> | Priority of a device in the VSU system, ranging from 1 to 255.                                                                                                                                              |

**Defaults** The default *priority\_num* is 100.

**Command Mode** config-vs-domain configuration mode

**Usage Guide** A larger value means a higher priority. The chassis with a higher priority is elected as the active chassis.

You can use this command in standalone mode or in VSU mode. The modified priority takes effect only after you restart the device.

In VSU mode, **switch\_id** indicates the ID of the running device. If the ID does not exist, the configuration does not effect.

**Configuration Examples** The following example sets the priority of device 1 to **200**.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# exit
```

The following example sets the priority of device 1 to **200** and restores the priority of device 2 to the default value in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# no switch 2 priority
Ruijie(config-vs-domain)# exit
```

| <b>Related<br/>Commands</b> | Command                    | Description                                                        |
|-----------------------------|----------------------------|--------------------------------------------------------------------|
|                             | <b>switch</b>              | Modifies the device ID in standalone mode.                         |
|                             | <b>show switch virtual</b> | Displays the domain ID as well as the ID and role of each chassis. |

**Platform**  
**Description**

N/A



## 9.21 switch renumber

Use this command to modify the ID of any device in VSU mode.

Use the **no** form of this command to restore the default setting.

**switch** *switch\_id* **renumber** *new\_switch\_id*

**no switch** *switch\_id*

| <b>Parameter<br/>Description</b> | Parameter            | Description                                                                                                                                                                                                    |
|----------------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | <i>switch_id</i>     | ID of the running device in VSU mode<br><br> The range depends on products. For details, see the <i>Configuration Guide</i> . |
|                                  | <i>new_switch_id</i> | ID of the new switch<br><br> The range depends on products. For details, see the <i>Configuration Guide</i> .               |

**Defaults**

N/A

**Command Mode**

config-vs-domain configuration mode

**Usage Guide**

This command is configured in VSU mode. In addition and takes affect after device restart.  
The **no** form of this command will restore the switch ID to 1.

**Configuration Examples**

The following example modifies the ID of device 1 that is running to 2 in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 renumber 2
```

The following example restores the ID of device 2 that is running to the default value in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# no switch 2
```

| <b>Related<br/>Commands</b> | Command                    | Description                                                        |
|-----------------------------|----------------------------|--------------------------------------------------------------------|
|                             | <b>switch</b>              | Modifies the device ID in standalone mode.                         |
|                             | <b>show switch virtual</b> | Displays the domain ID as well as the ID and role of each chassis. |

**Platform**  
**Description** N/A

## 9.22 switch virtual aggregateport lff enable

Use this command to enable the locally-preferred forwarding function on the AP in VSU mode.

Use the **no** form of this command to disable this function.

**switch virtual aggregateport lff enable**

**no switch virtual aggregateport lff enable**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** This function is enabled by default.

**Command Mode** config-vs-domain configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the locally-preferred forwarding function on the AP in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch virtual aggregateport lff enable
```

| Related Commands | Command                            | Description                                  |
|------------------|------------------------------------|----------------------------------------------|
|                  | <b>show switch virtual balance</b> | Displays the current traffic balancing mode. |

**Platform**  
**Description** N/A

## 9.23 switch virtual domain

Use this command to modify the domain ID of a device in standalone mode, or enter config-vs-domain configuration mode in VSU mode.

Use the **no** form of this command to restore the default setting.

**switch virtual domain *domain\_id***

**no switch virtual domain**

| Parameter          | Parameter        | Description                                       |
|--------------------|------------------|---------------------------------------------------|
| <b>Description</b> | <i>domain_id</i> | Domain ID of the VSU, in the range from 1 to 255. |

**Defaults** The default is 100.

**Command Mode** config-vs-domain configuration mode

**Usage Guide** Only two devices with the same domain ID can form a virtual device. The domain ID must be unique within the local area network (LAN).

**Configuration** The following example sets the domain ID of the VSU to 1 in standalone mode.

**Examples**

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)#
```

**Related****Commands**

| Command                    | Description                                                        |
|----------------------------|--------------------------------------------------------------------|
| <b>show switch virtual</b> | Displays the domain ID as well as the ID and role of each chassis. |
| <b>switch domain</b>       | Modifies the domain ID in VSU mode.                                |

**Platform****Description**

N/A

## 9.24 switch virtual ecmp lff enable

Use this command to enable the locally-preferred forwarding function on the ECMP interface in VSU mode.

Use the **no** form of this command to disable this function.

**switch virtual ecmp lff enable**

**no switch virtual ecmp lff enable**

**Parameter****Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

This function is enabled by default.

**Command Mode**

config-vs-domain configuration mode

**Usage Guide**

N/A

**Configuration****Examples**

The following example enables the locally-preferred forwarding function on the ECMP interface in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)#switch virtual ecmp lff enable
```

**Related****Commands**

| Command                            | Description                             |
|------------------------------------|-----------------------------------------|
| <b>show switch virtual balance</b> | Displays the current load balance mode. |

**Platform****Description**

N/A

## 9.25 vsl-port

Use this command to enter VSL-PORT mode

**vsl-port**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is configured on a device in whether standalone mode or VSU mode.

**Configuration** The following example enters VSL-AP configuration mode on a device in standalone mode.

**Examples**

```
Ruijie(config)# vsl-port
Ruijie(config-vsl-port)#
```

The following example enters VSL-APPOROT configuration mode on a device in VSU mode.

```
Ruijie(config)# vsl-port
Ruijie(config-vsl-port)#
```

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

**Platform**  
**Description** N/A

## 10 RNS &Track Commands

### 10.1 delay

Use this command to specify a period of time after which the tracked object status will change if the interface status changes.

Use the **no** form of this command to restore the default setting.

**delay** { **up** *seconds* [ **down** *seconds* ] | [ **up** *seconds* ] **down** *seconds* }

**no delay**

| Parameter Description | Parameter                  | Description                                                                         |
|-----------------------|----------------------------|-------------------------------------------------------------------------------------|
|                       | <b>up</b> <i>seconds</i>   | Sets the delay time from down to up in the range from 0 to 180. The unit is second. |
|                       | <b>down</b> <i>seconds</i> | Sets the delay time from up to down in the range from 0 to 180. The unit is second. |

**Defaults** There is no delay by default.

**Command Mode** Track configuration mode

**Usage Guide** The continual oscillation of the tracked object status may cause the client of this tracked object changing also. This command can be used to delay advertising the change of the tracked object status. For example, the status of a tracked object changes from up to down, if the delay down 180 is configured, the down status will be advertised after 180 seconds. If the tracked object status changes to the up again in this period, it won't be advertised. For the client of the tracked object, the status of the tracked object is always up.

**Configuration Examples** The following example sets the delay time to 30 seconds when the tracked object changes to up from down.

```
Ruijie(config)# track 5 rns 10
Ruijie(config-track)# delay up 30
Ruijie(config-track)# end
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 10.2 dns

Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode.

**dns** {*destination-hostname* **name-server** *a.b.c.d* [**source-ipaddr** *ip-address*] [**out-interface** *type num*] [**next-hop** *A.B.C.D*]} | **oob** *destination-hostname* **name-server** *a.b.c.d* [**source-ipaddr** *ip-address*] **via** *type num* **next-hop** *A.B.C.D*}

| Parameter Description | Parameter                            | Description                                                                                  |
|-----------------------|--------------------------------------|----------------------------------------------------------------------------------------------|
|                       | <i>destination-hostname</i>          | Sets the destination IP address or the destination host domain name.                         |
|                       | <b>oob</b>                           | Enables management port detection.                                                           |
|                       | <i>a.b.c.d</i>                       | Sets the IP address for the DNS server.                                                      |
|                       | <i>ip-address</i>                    | Indicates the source IP address of RNS packets.                                              |
|                       | <b>out-interface</b> <i>type num</i> | Specifies the egress interface (non-management port) for RNS packets.                        |
|                       | <b>via</b> <i>type num</i>           | Specifies the management port as the egress interface (non-management port) for RNS packets. |
|                       | <i>A.B.C.D</i>                       | Specifies the next-hop IP address for RNS packets.                                           |

**Defaults** N/A

**Command Mode** IP RNS configuration mode

**Usage Guide** Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode. If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

**Configuration Examples** The following example sets the IP RMS object to send the DNS packets.

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# dns www.ruijie.com.cn name-server 61.154.22.41
Ruijie(config-ip-rns-dns)# exit
Ruijie(config)# ip rns schedule 1 start-time now
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 10.3 frequency

Use this command to set the interval of sending the packets, which must be no smaller than the timeout time.

Use the **no** form of this command to restore the default setting.

**frequency** *milliseconds*

**no frequency**

| Parameter Description | Parameter           | Description                                                                                                |
|-----------------------|---------------------|------------------------------------------------------------------------------------------------------------|
|                       | <i>milliseconds</i> | Sets the interval of sending the packets, in the range from 10 to 604,800,000 in the unit of milliseconds. |

**Defaults** The default is 60 seconds.

**Command** IP RNS ICMP echo configuration mode

**Mode** IP RNS DNS configuration mode

IP RNS UDP echo configuration mode

**Usage Guide** Use this command to set the interval of sending the ICMP echo or DNS packets, which must accord with the following formula to ensure accuracy:

**frequency** *milliseconds* > **timeout** *milliseconds* >= **threshold** *milliseconds*

**Configuration** The following example configures an ICMP echo probe whose destination address is 192.168.21.1.

**Examples** The frequency, timeout time and threshold are set to 30,000, 8,000 and 6,000 milliseconds respectively.

```
Ruijie(config-ip-rns)#icmp-echo 192.168.21.1
Ruijie(config-ip-rns-icmp-echo)#frequency 30000
Ruijie(config-ip-rns-icmp-echo)#timeout 8000
Ruijie(config-ip-rns-icmp-echo)#threshold 6000
```

| Related Commands | Command        | Description                                      |
|------------------|----------------|--------------------------------------------------|
|                  | <b>timeout</b> | Defines the timeout time of sending the packets. |

**Platform** N/A

**Description**

## 10.4 icmp-echo

Use this command to configure an ICMP echo RNS probe.

**icmp-echo** { *destination-ip-address* | *destination-hostname* [ **name-server** *ip-address* ] }



```
[source-ipaddr ip-address] [out-interface type num [next-hop A.B.C.D]] | oob
{ destination-ip-address | destination-hostname [name-server ip-address] } [source-ipaddr
ip-address] via type num next-hop A.B.C.D
```

| Parameter Description | Parameter                              | Description                                                                                                      |
|-----------------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------|
|                       | <b>oob</b>                             | Enables management port detection.                                                                               |
|                       | <i>destination-hostname</i>            | Sets the destination host name within 127 characters. The exceeding characters are truncated automatically.      |
|                       | <b>name-server</b> <i>ip-address</i>   | Sets the domain name server. The default domain name server is configured via the <b>ip name-server</b> command. |
|                       | <b>source-ipaddr</b> <i>ip-address</i> | Sets the source IP address for the ICMP echo packets.                                                            |
|                       | <b>out-interface</b> <i>type num</i>   | Sets the egress port(non-management) for the probe packet.                                                       |
|                       | <b>via</b> <i>type num</i>             | Specifies the management port as the egress interface (non-management port) for probe packets.                   |
|                       | <b>next-hop</b> <i>A.B.C.D</i>         | Sets the next hop IP address.                                                                                    |

**Defaults** N/A

**Command Mode** IP RNS configuration mode

**Usage Guide** This command is used to enable the IP RNS object to send ICMP echo packets containing the specified destination IP address. The default payload size of an ICMP echo packet is 36 bytes. The **request-data-size** command is used to modify the packet size.

You can modify the probe parameter after specifying the type of the IP RNS probe (such as ICMP echo probe). If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

**Configuration Examples** The following example enables the IP RNS object to send the ICMP echo packets containing the destination IP address 10.1.1.1.

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 10.5 ip rns

Use this command to define an IP RNS operation object and to enter the IP RNS configuration mode.

Use the **no** form of this command to delete an IP RNS operation object.

**ip rns** *operation-number*

**no ip rns** *operation-number*

| Parameter Description | Parameter               | Description                                                          |
|-----------------------|-------------------------|----------------------------------------------------------------------|
|                       | <i>operation-number</i> | Sets the IP RNS operation object number, in the range from 1 to 500. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** Use this command to define an IP RNS operation object and to enter the IP RNS configuration mode. At present, IP RNS probe only supports IPv4 upon 500 objects at most, which depends on device performance. As a value-added feature, too much IP RNS probe may lead in system overload. As a result, it will be disabled for the time being, ensuring normal function of core services (e.g. routing). After the IP RNS configuration mode is enabled, the probe object will not be created unless the probe type is configured. If the type is set and object is created, use the **ip rns schedule** command to configure the startup policy, or the probe cannot be performed; use the **ip rns** command to enter the sub mode. If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

**Configuration** The following example defines the IP RNS object 1.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

| Related Commands | Command                       | Description                                         |
|------------------|-------------------------------|-----------------------------------------------------|
|                  | <b>show ip rns statistics</b> | Displays the statistical data on the IP RNS object. |

**Platform Description** N/A

## 10.6 ip rns reaction-configuration

Use this command to configure proactive threshold monitoring and trigger for the IP RNS probe.

Use the **no** form of this command to restore the default setting.

```
ip rns reaction-configuration operation-number react monitored-element [action-type option]
[threshold-type { average [number-of-measurements] | consecutive [occurrences] | immediate
| never | xofy [x-value y-value] }] [threshold-value upper-threshold lower-threshold]
no ip rns reaction-configuration operation-number [react monitored-element]
```

**Parameter  
Description**

| Parameter                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>operation-number</i>                                                    | Operation index, in the range from 1 to 500.                                                                                                                                                                                                                                                                                                                                                                                                        |
| <i>monitored-element</i>                                                   | <ul style="list-style-type: none"> <li>Monitored element. The available parameters are listed as follows:</li> <li><b>allfail</b>: Failed to monitor all elements. The default action-type is <b>track</b>. This parameter is applied on the track module for communication.</li> <li><b>rtt</b>: Packet round trip time (RTT) exceeds the threshold range.</li> <li><b>•timeout</b>: Timeout in whatever direction.</li> </ul>                     |
| <b>action-type</b> <i>option</i>                                           | <ul style="list-style-type: none"> <li>The available parameters include:</li> <li><b>none</b>: No action, which is the default setting</li> <li><b>trigger</b>: Only supports the <b>trigger</b> action.</li> <li><b>track</b>: Only supports the <b>track</b> action. Only when <b>monitored-element is allfail is this parameter supported, which is available exclusively.</b></li> </ul>                                                        |
| <b>average</b><br>[ <i>number-of-measurements</i> ]                        | Triggers operation when the average value of <b>number-of-measurements</b> consecutive times exceeds the threshold range. For example. <i>number-of-measurements</i> is set to three. Upper and lower thresholds are 5000 and 4000 respectively. <b>The average value for three consecutive measurements 6000. 6000. 5000 is (6000+6000+5000)/3=5667, exceeding the upper threshold 5000. The valid range is from 1 to 16 and the default is 5.</b> |
| <b>consecutive</b> [ <i>occurrences</i> ]                                  | Triggers operation when the value of monitored element exceeds the threshold range for <i>occurrences</i> consecutive times. The valid range is from 1 to 16. The default is 5.                                                                                                                                                                                                                                                                     |
| <b>immediate</b>                                                           | Triggers operation immediately when the value of monitored element exceeds the threshold range.                                                                                                                                                                                                                                                                                                                                                     |
| <b>never</b>                                                               | Never triggers operation.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>xofy</b> [ <i>x-value y-value</i> ]                                     | X probes among the latest Y ones exceed the threshold range. The valid X range is from 1 to 16 and the default is 5. The valid Y range is from 1 to 16 and the default is 5.                                                                                                                                                                                                                                                                        |
| <b>threshold-value</b><br><i>upper-threshold</i><br><i>lower-threshold</i> | Configures upper and lower thresholds.<br>When <i>monitored-element</i> is <b>rtt</b> , this parameter indicates time, in the range from 0 to 60,000 milliseconds. See <b>Usage Guide</b> for the default setting.                                                                                                                                                                                                                                  |

|  |                                                                         |
|--|-------------------------------------------------------------------------|
|  | When react type is timeout, you don't need to configure this parameter. |
|--|-------------------------------------------------------------------------|

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** One IP RNS object can be configured with multiple thresholds monitoring, each for one element. Monitored elements that are supported vary with different probe types.

| monitored-element | icmp-echo | dns | udp-echo |
|-------------------|-----------|-----|----------|
| timeout           | ✓         | ✓   | ✓        |
| rtt               | ✓         | ✓   | ✓        |

The default thresholds for monitored elements are listed as follows:

| Monitored Element | Upper Threshold | Lower Threshold |
|-------------------|-----------------|-----------------|
| timeout           | -               | -               |
| rtt               | 5000 ms         | 0 ms            |

**Configuration** The following example configures RNS1 and its threshold monitoring.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 192.168.23.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
Ruijie(config)# ip rns reaction-configuration 1 react timeout threshold-type
immediate action-type triggerOnly
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 10.7 ip rns reaction-trigger

Use this command to enable the IP RNS probe which exceeds the monitoring threshold to trigger another IP RNS probe which is in the pending state.

Use the **no** form of this command to restore the default setting.

**ip rns reaction-trigger** *operation-number target-operation*

**no ip rns reaction-trigger** *operation-number target-operation*

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|                         |                                                         |
|-------------------------|---------------------------------------------------------|
| <i>operation-number</i> | The source operation number, in the range from 1 to 500 |
| <i>target-operation</i> | The target operation number, in the range from 1 to 500 |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** The trigger function is applied in network fault diagnosis scenario

**Configuration** The following example enables IP RNS1 to trigger IP RNS 2.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo www.baidu.com
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)#ip rns schedule 1 start-time now life forever
Ruijie(config)#ip rns reaction-configuration 1 react timeout threshold-type
immediate action-type trigger
Ruijie(config)# ip rns 2
Ruijie(config-ip-rns)# dns www.baidu.com name-server 8.8.8.8
Ruijie(config-ip-rns-dns)# exit
Ruijie(config)#ip rns reaction-trigger 1 2
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 10.8 ip rns reset

Use this command to clear all IP RNS configuration.

**ip rns reset**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to clear all IP RNS configuration. This command is used only in extreme cases

(for example, RNS probe configuration is wrong).

**Configuration** The following example clears all IP RNS configuration.

**Examples**

```
Ruijie(config)# ip rns reset
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 10.9 ip rns restart

Use this command to restart the IP RNS probe.

**ip rns restart** *operation-number*

| Parameter Description | Parameter               | Description |
|-----------------------|-------------------------|-------------|
|                       | <i>operation-number</i> |             |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to restart the IP RNS probe whose schedule is in the pending state. This command is invalid for the IP RNS probe not configured with the scheduling policy.

**Configuration** The following example restarts IP RNS 1.

**Examples**

```
Ruijie(config)# ip rns restart 1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 10.10 ip rns schedule

Use this command to configure the scheduling strategy, start time and survival time for the IP RNS probe. Use the **no** form of this command to restore the default setting.

```
ip rns schedule operation-number [life { forever | seconds }] [start-time { hh:mm [:ss] [month
day | day month] | pending | now | after hh:mm:ss }] [recurring]
no ip rns schedule operation-number
```

**Parameter  
Description**

| Parameter               | Description                                                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <i>operation-number</i> | RNS operation index, in the range from 1 to 500                                                                             |
| <b>life forever</b>     | The RNS operation is valid forever.                                                                                         |
| <b>life seconds</b>     | The RNS survival time, measured in seconds                                                                                  |
| <i>hh:mm [ :ss ]</i>    | Defines the time when the operation starts,                                                                                 |
| <i>month</i>            | The month when the operation starts, in the range from January (Jan.) to December (Dec.). The default is the current month. |
| <i>day</i>              | The day when the operation starts, in the range from 1 to 31. The default is the current day.                               |
| <b>pending</b>          | The start time is pending.                                                                                                  |
| <b>now</b>              | The operation starts right now.                                                                                             |
| <b>after hh:mm:ss</b>   | The operation starts after hh hours, mm minutes and ss seconds.                                                             |
| <b>recurring</b>        | The operation starts automatically as scheduled every day.                                                                  |

**Defaults**

The IP RNS probe is in the pending state by default. In other words, the probe is not performed unless it is triggered by another RNS probe.

**Command  
Mode**

Global configuration mode

**Usage Guide**

The **ip rns schedule** command is used to configure the IP RNS probe with scheduling policy. Once the scheduling policy is configured, the RNS probe cannot be modified. You can modify the RNS probe after deleting the schedule with the **no ip rns schedule** command.

Life {seconds} refers to the survival time of the IP RNS probe. The probe will end after the survival time.

**Configuration**

The following example configures the RNS probe with scheduling policy.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

Once the scheduling policy is configured, the RNS probe cannot be modified. The RNS probe can be modified after the schedule is deleted.

```
Ruijie(config)# ip rns 1
Entry already running and cannot be modified
 (only can delete (no) and start over)
 (check to see if the probe has finished exiting)
Ruijie(config)# no ip rns schedule 1
Ruijie(config)# ip rns 1
```

```
Ruijie(config-ip-rns-icmp-echo)# exit
```

#### Related Commands

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 10.11 object

Use this command to add a tracked object to the object track list.

Use the **no** form of this command to delete a tracked object.

**object** *object-number* [ **not** ]

**no object** *object-number*

#### Parameter Description

| Parameter            | Description                                       |
|----------------------|---------------------------------------------------|
| <i>object-number</i> | Tracked object number, in the range from 1 to 700 |

**Defaults** No tracked object is configured by default.

**Command Mode** Track configuration mode

**Usage Guide** This command is used to add a tracked object to the object track list. The number of tracked objects is only restricted by the track list capacity.

**object** *object-number*: The tracked object must be in the up state for the track list to be in the up state.

**object** *object-number* not: track: The tracked object must be in the up state for the track list to be in the up state,

- This command is configured only in track configuration mode for the track list.
- The object cannot track itself.
- The objects cannot track each other. For example, if A tracks B, B cannot track A. Otherwise, both A and B are in oscillation.

**Configuration Examples** The following example adds tracked object 4 to the object track list. When object 1 is in the up state, 2 down, 3 up, object 4 is in the up state.

```
Ruijie(config)# track 4 list boolean and
Ruijie(config-track)# object 1
Ruijie(config-track)# object 2 not
Ruijie(config-track)# object 3
```



```
Ruijie(config-track)# end
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform N/A

Description

## 10.12 request-data-size

Use the following example to set the protocol payload size of IP RNS probe packet.

Use the **no** form of this command to restore the default setting.

**request-data-size** *bytes*

**no request-data-size**

| Parameter Description | Parameter | Description  |
|-----------------------|-----------|--------------|
|                       |           | <i>bytes</i> |

**Defaults** The default is the minimum payload byte, which varies with the probe type.

**Command** IP RNS ICMP echo configuration mode

**Mode** IP RNS UDP echo configuration mode

**Usage Guide** This command is used to fill bytes in the probe packet to probe for the bigger packet.

| Probe Type | Range        | Default |
|------------|--------------|---------|
| icmp-echo  | [ 36, 1472 ] | 36      |
| Udp-echo   | [36, 1472]   | 36      |

**Configuration** The following example sets the protocol payload size of the IP RNS probe packet to 50.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# request-data-size 50
Ruijie(config-ip-rns-icmp-echo)# exit
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform N/A

Description

## 10.13 show ip rns configuration

Use this command to display the RNS instance configuration.

**show ip rns configuration** [ *operation-number* ]

| Parameter Description | Parameter               | Description                                               |
|-----------------------|-------------------------|-----------------------------------------------------------|
|                       | <i>operation-number</i> | Sets the RNS instance number, in the range from 1 to 500. |

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the RNS instance configuration. The configuration varies with different packet types.

**Configuration** The following example displays the RNS 1 configuration.

### Examples

```
Ruijie# show ip rns configuration 1
Entry number: 1
Tag: ruijie555
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 10000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): 3500
Next Scheduled Start Time:Start Time already passed
Target address/Source address: 2.2.2.3/0.0.0.0
Request size (ARR data portion): 36
```

| Field                              | Description                     |
|------------------------------------|---------------------------------|
| Entry number                       | IP RNS operation index          |
| Tag                                | Instance tag.                   |
| Type of operation to perform       | Operation type.                 |
| Operation timeout (milliseconds)   | Operation timeout.              |
| Operation frequency (milliseconds) | Operation frequency.            |
| Threshold (milliseconds)           | Threshold.                      |
| Recurring (Starting Everyday)      | The operation starts every day. |
| Life (seconds)                     | Life time                       |
| Next Scheduled Start Time          | Next scheduled start time.      |
| Target address/Source address      | Target address/Source address   |
| Request size (ARR data portion)    | Request packet size.            |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|------------------|---------|-------------|

|     |     |
|-----|-----|
| N/A | N/A |
|-----|-----|

**Platform** N/A

**Description**

## 10.14 show ip rns collection-statistics

Use this command to display statistics about the RNS probe.

**show ip rns collection-statistics** [ *operation-number* ]

| Parameter Description | Parameter               | Description                                                                                                       |
|-----------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------|
|                       | <i>operation-number</i> | Sets the IP RNS operation object number, in the range from 1 to 500. The default is all IP RNS operation objects. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display statistics about an IP RNS probe.

**Configuration** The following example displays statistics about the all RNS probes.

### Examples

```
Ruijie#show ip rns collection-statistics 1
Entry number: 1
Start Time Index: *2014-03-20 19:53:51
Number of successful operations: 919
Number of operations over threshold: 0
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 2
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 2
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
RTT Values:
RTTAvg: 18 RTTMin: 16 RTTMax: 37
NumOfRTT: 919 RTTSum: 16654 RTTSum2: 302786
```

| Field                                | Description                     |
|--------------------------------------|---------------------------------|
| Entry number                         | IP RNS operation index          |
| Start Time Index:                    | Schedule start time             |
| Number of successful operations:     | Number of successful operation. |
| Number of operations over threshold: | Number of threshold violation   |

|                                                       |                                                        |
|-------------------------------------------------------|--------------------------------------------------------|
| Number of failed operations due to a Disconnect:      | Number of operation failure due to disconnection       |
| Number of failed operations due to a Timeout:         | Number of operation failure due to timeout             |
| Number of failed operations due to a Busy:            | Number of operation failure since the peer end is busy |
| Number of failed operations due to a No Connection:   | Number of operation failure due to no connection       |
| Number of failed operations due to an Internal Error: | Number of operation failure due to internal error      |
| Number of failed operations due to a Sequence Error:  | Number of operation failure due to sequence error      |
| Number of failed operations due to a Verify Error:    | Number of operation failure due to verification error  |
| RTT Values                                            | RTT value                                              |
| RTTAvg:                                               | Average RTT value                                      |
| RTTMin:                                               | Minimum RTT value                                      |
| RTTMax:                                               | Maximum RTT value                                      |
| NumOfRTT:                                             | Number of counting RTT value                           |
| RTTSum:                                               | Sum of RTT value                                       |
| RTTSum2:                                              | Sum of squares of RTT value                            |

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A

## 10.15 show ip rns operational-state

Use this command to display operational state.

**show ip rns operational-state** [ *operation-number* ]

**Parameter  
Description**

| Parameter               | Description                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------|
| <i>operation-number</i> | Sets the IP RNS operation object number, in the range from 1 to 500. The default is all RNS operation objects. |

**Defaults**

N/A

**Command  
Mode**

Privileged EXEC mode

**Usage Guide** This command is used to display the state information about an RNS probe.

**Configuration** The following example displays the state information about all RNS probes.

**Examples**

```
Ruijie# show ip rns operational-state
Entry number: 1
Modification time: *2014-01-10 10:26:14
Current seconds left in Life: Forever
Operational state of entry: Active
Number of Octets Used by this Entry: 2272
Number of operations attempted: 232
Number of operations skipped: 0
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 4
Latest operation start time: 2014-01-10 10:26:55
Latest operation return code: OK
```

| Field                               | Description                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------------------|
| Entry number                        | IP RNS operation index                                                                      |
| Modification time                   | Probe result recounting time (every time schedule is enabled, the result is counted again). |
| Number of Octets Used by this Entry | Number of octets contained in the probe packet.                                             |
| Number of operations attempted      | Number of attempted operation.                                                              |
| Number of operations skipped        | Number of failed operation.                                                                 |
| Current seconds left in Life        | Probes for the left life.                                                                   |
| Operational state of entry          | Probes for the operational state (Active/Disactive).                                        |
| Connection loss occurred            | Connection loss occurred.                                                                   |
| Timeout occurred                    | Send request timeout occurred,                                                              |
| Over thresholds occurred            | Threshold violation occurred.                                                               |
| Latest RTT (milliseconds)           | Latest RTT.                                                                                 |
| Latest operation start time         | Latest operation start time.                                                                |
| Latest operation return code        | Latest operation return code.                                                               |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 10.16 show ip rns reaction-configuration

Use this command to display the proactive threshold monitoring information of an IP RNS probe.

**show ip rns reaction-trigger** [ *operation-number* ]

| Parameter Description | Parameter               | Description                                                                                                   |
|-----------------------|-------------------------|---------------------------------------------------------------------------------------------------------------|
|                       | <i>operation-number</i> | The number of IP RNS operation objects, in the range from 1 to 500. The default is all RNS operation objects. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the proactive threshold monitoring information of an IP RNS probe.

**Configuration Examples** The following example displays the proactive threshold monitoring information of all IP RNS probes.

```
Ruijie#show ip rns reaction-configuration
```

```
Entry number: 1
```

```
Reaction: rtt
```

```
Threshold Type: Never
```

```
Rising (milliseconds): 5000
```

```
Falling (milliseconds): 3000
```

```
Threshold Count: 5
```

```
Threshold Count2: 5
```

```
Action Type: trigger
```

```
Reaction: timeout
```

```
Threshold Type: Never
```

```
Threshold Count: 5
```

```
Threshold Count2: 5
```

```
Action Type: trigger
```

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entry number   | IP RNS operation index                                                                                                                                                                                                                                                                                                                                                                         |
| Reaction       | Monitored object                                                                                                                                                                                                                                                                                                                                                                               |
| Threshold Type | The available parameters are listed as follows:<br><b>never</b> : Never triggers operation.<br><b>consecutive</b> : Triggers operation when the value of monitored element exceeds the threshold range for <i>occurrences</i> consecutive times.<br><b>average</b> : Triggers operation when the average value of <b>number-of-measurements consecutive times</b> exceeds the threshold range. |

|                        |                                                                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | <p><b>immediate:</b> Triggers operation immediately when the value of monitored element exceeds the threshold range.</p> <p><b>xofy:</b> X probes among the latest Y ones exceed the threshold range.</p> |
| Rising (milliseconds)  | Upper threshold                                                                                                                                                                                           |
| Falling (milliseconds) | Lower threshold                                                                                                                                                                                           |
| Threshold Count        | The parameter refers to the x value when the threshold-type is <b>xofy</b> or the average count when the threshold-type is <b>average</b> .                                                               |
| Threshold Count2       | The parameter refers to the y value when the threshold-type is <b>xofy</b> or the consecutive count when the threshold-type is <b>consecutive</b> .                                                       |
| Action Type            | Action type                                                                                                                                                                                               |

#### Related Commands

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 10.17 show ip rns reaction-trigger

Use this command to display the reaction trigger information for all RNS objects.

**show ip rns reaction-trigger** [ *operation-number* ]

#### Parameter Description

| Parameter               | Description                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------|
| <i>operation-number</i> | The number of IP RNS operation object, in the range from 1 to 500.<br>The default is all RNS operation objects. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the reaction trigger information for all RNS objects.

**Configuration** The following example displays the reaction trigger information for all RNS objects.

**Examples**

```
Ruijie#show ip rns reaction-trigger
Entry number: 1
Target rns index: 2
```

Status of Entry (SNMP RowStatus): active

Operational State: pending

| Field                            | Description            |
|----------------------------------|------------------------|
| Entry number                     | RNS index              |
| Target rns index                 | Target RNS index       |
| Status of Entry (SNMP RowStatus) | Status of RNS entry    |
| Operational State                | Reaction-trigger state |

#### Related Commands

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

Platform N/A

Description

## 10.18 show ip rns statistics

Use this command to display the RNS object statistics.

**show ip rns statistics** [ *operation-number* ]

#### Parameter Description

| Parameter               | Description                                                         |
|-------------------------|---------------------------------------------------------------------|
| <i>operation-number</i> | Sets the IP RNS operation object number, in the range from 1 to 500 |

Defaults N/A

Command Privileged EXEC mode  
Mode

Usage Guide The statistics vary with different packet types.

Configuration The following example displays the RNS object statistics.

#### Examples

```
Ruijie#show ip rns statistics 1
Round trip time(RTT) Index 1
Operation time to live: Forever
Latest RTT: 1 ms
Latest operation start time: 2014-01-20 10:21:38
Latest operation return code: OK
Number of successes: 386
Number of failures: 12
```



| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 10.19 show track

Use this command to display statistics of the tracked object.

**show track** [ *track-number* ]

| Parameter Description | Parameter | Description         |
|-----------------------|-----------|---------------------|
|                       |           | <i>track-number</i> |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays statistics of all tracked objects.

```
Ruijie#show track
Track 1
 Reliable Network Service 5
 The state is Up
 1 change, current state last: 120 secs
 Delay up 30 secs, down 50 secs
Track 3
 Interface FastEthernet 1/0
 The state is Down, delayed Up (5 secs remaining)
 3 change, current state last: 300 secs
 Delay up 60 secs, down 60 secs
Track 4
 List boolean and
 Object 1
 Object 2 not
 The state is Up
 1 change, current state last: 100 secs
 Delay up 0 secs, down 0 secs
```

| Field   | Description       |
|---------|-------------------|
| Track x | Tracked object ID |

|                                              |                                                                     |
|----------------------------------------------|---------------------------------------------------------------------|
| Reliable Network Service x                   | Tracked RNS object                                                  |
| The state is x                               | Tracked object state                                                |
| x change                                     | Tracked object change count                                         |
| current state last: x secs                   | The time for which the current state lasts                          |
| Delay up x secs, down x secs                 | The delay state of the tracked object                               |
| Interface x x                                | Tracked interface                                                   |
| The state is x, delayed y (c secs remaining) | The tracked object state is x, and will turn to y in c seconds.     |
| List boolean and                             | The Boolean expression enables calculation by using “and” operator. |
| Object x                                     | Object x is in the up state.                                        |
| Object x not                                 | Object x is in the down state.                                      |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 10.20 show track client

Use this command to display the track client statistics.

**show track client****Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the statistics of the client connecting to track.

**Configuration Examples** The following example displays the statistics of the client connecting to track.

**Examples**

```
Ruijie# show track client
Track client 2: socket 4
client_path: /tmp/vsd/0/track/.client_nsm
Connection time: Fri Dec 28 17:04:43 2012
```

| Field | Description |
|-------|-------------|
|-------|-------------|

|                                           |                                            |
|-------------------------------------------|--------------------------------------------|
| Track client x: socket x                  | Track client number and socket             |
| client_path: /tmp/vsd/0/track/.client_nsm | The path from the client to track          |
| Connection time: xx xx xx xx:xx:xx xx     | The time when the client connects to track |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 10.21 tag

Use this command to set the tag for IP RNS probe.

Use the **no** form of this command to restore the default setting.

**tag** *text*

**no tag**

| Parameter Description | Parameter   | Description |
|-----------------------|-------------|-------------|
|                       | <i>text</i> |             |

**Defaults** N/A

**Command** IP RNS DNS configuration mode

**Mode** IP RNS ICMP echo configuration mode

IP RNS UDP echo configuration mode

**Usage Guide** Tag is used to identify the probe. When the tag exceeds 79 characters, the surplus characters are truncated.

**Configuration** The following example sets the tag for IP RNS probe to telecom gateway.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# tag telecom_gateway
Ruijie(config-ip-rns-icmp-echo)# exit
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 10.22 threshold

Use this command to configure the upper threshold value for IP RNS probe.

Use the **no** form of this command to restore the default setting.

**threshold** *milliseconds*

**no threshold**

**Parameter  
Description**

| Parameter           | Description                                                                                |
|---------------------|--------------------------------------------------------------------------------------------|
| <i>milliseconds</i> | Sets the upper threshold value, in the range from 0 to 60,000 in the unit of milliseconds. |

**Defaults**

The default is 5,000 milliseconds.

**Command**

IP RNS DNS configuration mode

**Mode**

IP RNS ICMP echo configuration mode

IP RNS P echo configuration mode

**Usage Guide**

The threshold value must be no greater than the timeout value. See **Usage Guide** of the **frequency** command for the relationship among timeout, frequency and threshold.

**Configuration**

The following example sets the upper threshold value for IP RNS probe to 8,000 milliseconds.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# threshold 8000
Ruijie(config-ip-rns-icmp-echo)# exit
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 10.23 timeout

Use this command to set the timeout time of an IP RNS probe.

Use the **no** form of this command to restore the default setting.

**timeout** *milliseconds*

**no timeout**

| Parameter Description | Parameter           | Description                                                                                                                |
|-----------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------|
|                       | <i>milliseconds</i> | Sets the timeout time, in the range from 10 to 604,800,000 in the unit of milliseconds. The default is 5,000 milliseconds. |

**Defaults** The default timeout of an IP RNS probe varies with the detection type, which can be displayed by using **show ip rns configuration** command.

**Command** IP RNS ICMP echo configuration mode

**Mode** IP RNS DNS configuration mode

IP RNS configuration mode

**Usage Guide** The timeout value must be no smaller than the threshold value. See **Usage Guide** of the **frequency** command for the relationship among timeout, frequency and threshold.

**Configuration** The following example sets the timeout time of an IP RNS probe to 10,000 milliseconds.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# timeout 10000
Ruijie(config-ip-rns-icmp-echo)# exit
```

| Related Commands | Command                              | Description                               |
|------------------|--------------------------------------|-------------------------------------------|
|                  | <b>frequency</b> <i>milliseconds</i> | Sets the interval of sending the packets. |

**Platform** N/A

**Description**

## 10.24 tos

Use this command to set the Type of Service (ToS) field in the IPv4 header of an IP RNS probe packet.

Use the **no** form of this command to restore the default setting.

**tos** *number*

**no tos**

| Parameter Description | Parameter     | Description                                                                                  |
|-----------------------|---------------|----------------------------------------------------------------------------------------------|
|                       | <i>number</i> | Sets the ToS field in the IPv4 header of an IP RNS probe packet, in the range from 0 to 255. |

**Defaults** The default is 0.

**Command** IP RNS DNS configuration mode

**Mode** IP RNS ICMP echo configuration mode  
IP RNS UDP echo configuration mode

**Usage Guide** ToS is an 8-bit field of an IPv4 packet. ToS can be used to set probe packet priority. Different ToS corresponds to different priority.

**Configuration** The following example sets the ToS field in the IPv4 header of an IP RNS probe packet to 128.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# tos 128
Ruijie(config-ip-rns-icmp-echo)# exit
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 10.25 track interface line-protocol

Use this command to configure a tracked object to track the interface status and enter the track mode.

Use the **no** form of this command to delete a tracked object.

**track** *object-number* **interface** *interface-type interface-number* **line-protocol**

**no track** *object-number*

**Parameter  
Description**

| Parameter                                        | Description                                               |
|--------------------------------------------------|-----------------------------------------------------------|
| <i>object-number</i>                             | Sets the tracked object number, in the range of 1 to 700. |
| <i>interface-type</i><br><i>interface-number</i> | Sets the interface type and the interface number.         |

**Defaults** N/A

**Command** Global configuration mode  
**Mode**

**Usage Guide** This command is used to configure a tracked object to track the link state of the interface. If the link state of the interface is up, the state of the corresponding tracked object is up too.

**Configuration** The following example configures the object “track 3” to track the link state of ethernet 0/1.

**Examples**

```
Ruijie(config)# track 3 interface ethernet 0/1 line-protocol
```

| Related Commands | Command           | Description                                                                 |
|------------------|-------------------|-----------------------------------------------------------------------------|
|                  | <b>track rns</b>  | Configures a tracked object to track the operating status of an rns object. |
|                  | <b>show track</b> | Displays the tracked object related information.                            |

Platform N/A

Description

## 10.26 track list

Use this command to configure a tracked list object and specify the state of the tracked list based on a Boolean calculation.

Use the **no** form of this command to restore the default setting.

**track** *object-number* **list boolean { and | or }**

**no track** *object-number*

| Parameter Description | Parameter | Description          |
|-----------------------|-----------|----------------------|
|                       |           | <i>object-number</i> |

Defaults N/A

Command Mode Global configuration mode

**Usage Guide** This command is used to configure a tracked list object and specify the state of the tracked list based on a Boolean calculation

- **track** *object-number* **list boolean and**: Configure a tracked list with a Boolean expression using “AND” operator.
- **track** *object-number* **list boolean or**: Configure a tracked list with a Boolean expression using “OR” operator.

**Configuration Examples** The following example configures tracked list object “4” and specifies the state of the tracked list based on a Boolean calculation using operator “AND”.

```
Ruijie(config)# track 4 list boolean and
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  |         | N/A         |

Platform N/A

Description

## 10.27 track rns

Use this command to configure a tracked object to track the operating status of an RNS object and enter the track mode.

Use the **no** form of this command is used to delete a tracked object.

**track** *object-number* **rns** *entry-number*

**no track** *object-number*

### Parameter Description

| Parameter            | Description                                                 |
|----------------------|-------------------------------------------------------------|
| <i>object-number</i> | Sets the tracked object number, in the range from 1 to 700. |
| <i>entry-number</i>  | Sets the RNS object number, in the range from 1 to 500.     |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** The RNS object status is determined by whether the response packets are received. If so, the RNS object status is up and the status of the corresponding tracked object that tracks this RNS is also up.

**Configuration Examples** The following example configures the object “track 5” to track the RNS instance “rns 7”.

```
Ruijie(config)# track 5 rns 7
```

### Related Commands

| Command                                   | Description                                                  |
|-------------------------------------------|--------------------------------------------------------------|
| <b>track interface line-protocol</b>      | Tracks the status of one interface and enter the track mode. |
| <b>show track</b> [ <i>track-number</i> ] | Displays the tracked object related information.             |

**Platform Description** N/A

## 10.28 vrf

Use this command to set the VRF where the IP RNS probe resides.

Use the **no** form of this command to restore the default setting.

**vrf** *vrf-name*

**no vrf**

### Parameter Description

| Parameter       | Description        |
|-----------------|--------------------|
| <i>vrf-name</i> | Sets the VRF name. |



**Defaults** N/A

**Command** IP RNS ICMP echo configuration mode

**Mode** IP RNS DNS configuration mode

IP RNS UDP echo configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the VRF where the IP RNS probe resides to VPN1.

**Examples**

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 192.168.23.1
Ruijie(config-ip-rns-icmp-echo)# vrf VPN1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

**Related  
Commands**

| Command                              | Description                               |
|--------------------------------------|-------------------------------------------|
| <b>frequency</b> <i>milliseconds</i> | Sets the interval of sending the packets. |

**Platform** N/A

**Description**

# 11 VSD Commands

## 11.1 allocate interface

Use this command to allocate physical port resources to the VSD.

**allocate interface** *int\_index*

Use the **no** form of this command to reclaim physical ports allocated to a non-default VSD.

**no allocate interface** *int\_index*

### Parameter Description

| Parameter                         | Description              |
|-----------------------------------|--------------------------|
| <b>interface</b> <i>int_index</i> | Labels of physical ports |

### Defaults

All physical ports belong to the default VSD, also known as VSD0.

### Command Mode

VSD configuration mode

### Usage Guide

This command is used to allocate or reclaim physical ports to or from a non-default VSD.



If no physical port is available for a non-default VSD, the VSD can only be managed but not used. If all physical ports are allocated to a non-default VSD, the default VSD will have no physical port available. The VSL interface cannot be allocated.

### Configuration

The following example allocates physical ports to a non-default VSD (named admin).

### Examples

```
Ruijie# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vsd admin
Ruijie(config-vsd)#allocate interface tenGigabitEthernet 2/2/44
Interface-group[2/2/1 ~ 2/2/44] and their config will be removed from vsd[0].
Are you sure to continue(y/n)? [no]y
Allocating ports of slot 2/2 may lead to topological division because of vsl
port on this card.Are you sure to continue(y/n)? [no]y
```

### Platform

N/A

### Description

## 11.2 allocate slot

Use this command to allocate multi-service card resources to a VSD.

Use the **no** form of this command to reclaim multi-service card resources allocated to a non-default VSD.

**allocate slot** *slot\_id*  
**no allocate slot** *slot\_id*

**Parameter  
Description**

| Parameter                  | Description                     |
|----------------------------|---------------------------------|
| <b>slot</b> <i>slot_id</i> | Slot ID of a multi-service card |

**Defaults**

Multi-service cards belong to the default VSD, also known as VSD0.

**Command Mode**

VSD configuration mode

**Usage Guide**

This command is used to allocate multi-service card resources to a non-default VSD or to reclaim multi-service card resources from the non-default VSD.

**Configuration**

The following example allocates multi-service cards to a non-default VSD (named admin).

**Examples**

```
Ruijie# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vsd admin
Ruijie(config-vsd)# allocate slot 1/2
Allocating slot 1/2 may cause some service in source vsd to stop. Are you sure
to continue (y/n)? [no]y
Ruijie(config-vsd)#
```

**Platform**

N/A

**Description**

## 11.3 show vsd

Use this command to display the VSD information.

**show vsd** { **current-vsd** | { { **membership** | **detail** | **all** } [ *vsd\_name* ] } }

**Parameter  
Description**

| Parameter          | Description                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>current-vsd</b> | Name and ID of the current VSD                                                                                                     |
| <b>membership</b>  | Displays physical port resources and multi-service resources in a VSD.                                                             |
| <b>detail</b>      | Displays detailed information about a VSD including its ID, name and MAC address.                                                  |
| <b>all</b>         | Displays full information about a VSD including its ID, name and MAC address, physical port resources and multi-service resources. |
| <i>vsd_name</i>    | Specifies a VSD. It refers to a VSD0, by default.                                                                                  |

**Command Mode**

Privileged EXEC mode/Global configuration mode

**Usage Guide** This command is used to display the information about VSD's physical port resources, multi-card resources and MAC address resources and etc.

**Configuration** The following example displays the ID and name of the current VSD.

**Examples**

```
Ruijie# sho vsd current-vsds
Current vsd is 1 -Default
Ruijie #
```

**Field Description**

| Field            | Description             |
|------------------|-------------------------|
| Current vsd is 0 | ID of the current VSD   |
| Default          | Name of the current VSD |

The following example displays physical port resources and multi-service resources in all the VSDs.

```
Ruijie(config)# show vsd membership
vsd_id: 0
vsd_name: Default
interface:
TenGigabitEthernet 1/1 TenGigabitEthernet 1/2
 TenGigabitEthernet 1/3 TenGigabitEthernet 1/4
 TenGigabitEthernet 1/5 TenGigabitEthernet 1/6
 TenGigabitEthernet 1/7 TenGigabitEthernet 1/8

slot:
NA

vsd_id: 1
vsd_name: production
interface:
NA
slot:
NA
```

**Field Description**

| Field     | Description                  |
|-----------|------------------------------|
| vsd_id    | ID of a VSD                  |
| vsd_name  | Name of a VSD                |
| interface | Physical port resources      |
| slot      | Multi-service card resources |

The following example displays detailed information about all the VSDs.

```
Ruijie# show vsd detail
vsd_id: 0
vsd_name: Default
mac address: 00d0.f822.33c2
```

```

memory ratio: 70%
cpu weight: 10

memory:
Dev Slot Total (MB) Quota (MB) Used (MB) Available (MB)
--- ---
1 M1 4000 4000 900 3000
1 M2 4000 4000 700 3200

cpu:
Dev Slot Weight Usage (%)
--- ---
1 M1 10 5
1 M2 10 3

vsd_id: 1
vsd_name: production
mac address: 00d0.f822.33c3
memory ratio: 30%
cpu weight: 10

memory:
Dev Slot Total (MB) Quota (MB) Used (MB) Available (MB)
--- ---
1 M1 4000 900 200 700
1 M2 4000 900 100 800

cpu:
Dev Slot Weight Usage (%)
--- ---
1 M1 10 1
1 M2 10 1

```

## Field Description

| Field        | Description                      |
|--------------|----------------------------------|
| vsd_id       | VSD ID                           |
| vsd_name     | VSD name                         |
| mac address  | VSD MAC address                  |
| memory ratio | Maximum memory ratio             |
| cpu weight   | Maximum CPU weight               |
| memory       | Memory usage on different boards |
| Dev          | Device number                    |
| Slot         | Slot number                      |
| Total        | Total memory (MB)                |
| Quota        | Allocated memory (MB)            |

|           |                               |
|-----------|-------------------------------|
| Used      | Used memory (MB)              |
| Available | Idle memory (MB)              |
| cpu       | CPU usage on different boards |
| Weight    | Used CPU weight               |
| Usage     | Used CPU ratio (%)            |

The following example displays the whole information about a VSD.

```
Ruijie#show vsd all
vsd_id: 0
vsd_name: Default
vsd mac address: 00d0.f822.33c0
memory ratio: 70%
cpu weight: 10

memory:
Dev Slot Total (MB) Quota (MB) Used (MB) Available (MB)
--- ---
1 M1 4000 4000 900 3000
1 M2 4000 4000 700 3200

cpu:
Dev Slot Weight Usage (%)
--- ---
1 M1 10 5
1 M2 10 3

interface:
 TenGigabitEthernet 2/2/1 TenGigabitEthernet 2/2/2
 TenGigabitEthernet 2/2/3 TenGigabitEthernet 2/2/4
 TenGigabitEthernet 2/2/5 TenGigabitEthernet 2/2/6
 TenGigabitEthernet 2/2/7 TenGigabitEthernet 2/2/8

slot:
 NA

vsd_id: 1
vsd_name: vsd1
vsd mac address: 00d0.f822.33c2
memory ratio: 30%
cpu weight: 10

memory:
Dev Slot Total (MB) Quota (MB) Used (MB) Available (MB)
```

```

1 M1 4000 900 200 700
1 M2 4000 900 100 800

cpu:
Dev Slot Weight Usage (%)

1 M1 10 1
1 M2 10 1

interface:
 NA

slot:
 NA

```

## Field Description

| Field           | Description                      |
|-----------------|----------------------------------|
| vsd_id          | VSD ID                           |
| vsd_name        | VSD name                         |
| vsd mac address | VSD MAC address                  |
| memory ratio    | Maximum memory ratio             |
| cpu weight      | Maximum CPU weight               |
| interface       | Physical interface resource      |
| slot            | Multi-service card resource      |
| memory          | Memory usage on different boards |
| Dev             | Device number                    |
| Slot            | Slot number                      |
| Total           | Total memory (MB)                |
| Quota           | Allocated memory (MB)            |
| Used            | Used VSD memory (MB)             |
| Available       | Idle memory (MB)                 |
| cpu             | CPU usage on different boards    |
| Weight          | Used CPU weight                  |
| Usage           | Used CPU ratio (%)               |

**Platform**  
**Description**

N/A

## 11.4 switchback

Use this command to switch back from the non-default VSD to the default VSD.

**switchback**

| <b>Parameter Description</b>  | Parameter                                                                                                                                                                                                                                                                                                                                                | Description |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|                               | N/A                                                                                                                                                                                                                                                                                                                                                      | N/A         |
| <b>Command Mode</b>           | Privileged EXEC mode                                                                                                                                                                                                                                                                                                                                     |             |
| <b>Level</b>                  | 14                                                                                                                                                                                                                                                                                                                                                       |             |
| <b>Usage Guide</b>            | This command is used to switch back from a non-default VSD to the default VSD. This command does not support login to the non-default VSD via Telnet, which means that this command is effective only when switching from the default VSD to the non-default VSD (that is to say, switchto shall go before switchback).                                  |             |
| <b>Configuration Examples</b> | <p>The following example switches back from a non-default VSD (named admin) to the default VSD.</p> <pre>Ruijie# switchto vsd admin ***** Ruijie General Operating System Software Copyright (c) 1998-2013s by Ruijie Networks. All Rights Reserved. Neither Decompiling Nor Reverse Engineering Shall Be Allowed. ***** admin# switchback Ruijie#</pre> |             |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                                                                                                                                                                      |             |

## 11.5 switchto vsd

Use this command to log in from the default VSD to a non-default VSD.

**switchto vsd** *vsd\_name*

| <b>Parameter Description</b> | Parameter                                                                              | Description               |
|------------------------------|----------------------------------------------------------------------------------------|---------------------------|
|                              | <b>vsd</b> <i>vsd_name</i>                                                             | Name of a non-default VSD |
| <b>Command Mode</b>          | Privileged EXEC mode                                                                   |                           |
| <b>Level</b>                 | 14                                                                                     |                           |
| <b>Usage Guide</b>           | This command is used to log in from the default VSD to a non-default VSD.              |                           |
| <b>Configuration</b>         | The following example logs in from the default VSD to a non-default VSD (named admin). |                           |



**Examples**

```
Ruijie# switchto vsd admin

Ruijie General Operating System Software
Copyright (c) 1998-2013s by Ruijie Networks.
All Rights Reserved.
Neither Decompiling Nor Reverse Engineering Shall Be Allowed.

admin#
```

**Platform**

N/A

**Description**

## 11.6 vsd

Use this command to create a VSD or just enter the VSD configuration mode (if a VSD has been created).

**vsd** *vsd\_name* [**id** *vsd\_number*]

Use the **no** form of this command to delete a created a non-default VSD.

**no vsd** *vsd\_name*

**Parameter Description**

| Parameter                   | Description                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>vsd</b> <i>vsd_name</i>  | Name of a non-default VSD                                                                                                     |
| <b>id</b> <i>vsd_number</i> | No. of a VSD When no parameter is specified, the system will automatically allocate the smallest number available to the VSD. |

**Defaults**

No non-default VSD is created by default.


**Command Mode**

Global configuration mode

**Usage Guide**

This command is used to create a VSD and enter the VSD configuration mode. If a VSD has been created, use this command to enter the VSD configuration mode.

When entering the specified VSD configuration mode, you do not need to enter the vsd\_number. If you enter the vsd\_number, make sure that it is consistent with the current VSD number; otherwise, an error message appears.

 Get a corresponding license before you create a non-default VSD, with the total number of non-default VSDs created not greater than the total authorized number. The name of a VSD is independent from and irrelevant to the hostname of the device.

**Configuration Examples**

The following example creates a non-default VSD (named admin).

**Examples**

```
Ruijie# con t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Ruijie(config)# vsd admin
Note: Creating VSD, one moment please ...
Ruijie(config-vsd)#
```

The following example enters the VSD configuration mode if a non-default VSD (named admin) has been created.

```
Ruijie# con t
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# vsd admin
Ruijie(config-vsd)#
```

The following example deletes a non-default VSD (named admin).

```
Ruijie# con t
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# no vsd admin
Deleting this vsd will remove its config. Continue to delete this vsd(y/n)? [no]y
Allocating ports of slot 2/2 may lead to topological division because of vsl
port on this card.Are you sure to continue(y/n)? [no]y
Note: Deleting VSD, one moment please ...
Ruijie(config)#
```

**Platform**  
**Description**

N/A

## 12 NLB GROUP Commands

### 12.1 nlb-group

Use this command to create a cluster group and specify the cluster's attributes (VRF, IP address and reflector port) or the port connecting the cluster with device.

Use the **no** form of this command to delete the cluster's attributes or delete the port connecting with the cluster separately.

**nlb-group** *group-number* [ **vrf** *vrf-name* ] **ip** *nlb-address* [ **reflector-port** *interface-name* ]

**nlb-group** *group-number* **destination-port** *interface-name*

**no nlb-group** *group-number* [ [ **vrf** *vrf-name* ] **ip** *nlb-address* [ **reflector-port** *interface-name* ] ]

**no nlb-group** *group-number* [ **destination-port** *interface-name* ]

**no nlb-group all**

#### Parameter Description

| Parameter                                        | Description                                                                                                                                                                                                          |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nlb-group</b> <i>group-number</i>             | Cluster group number                                                                                                                                                                                                 |
| <b>vrf</b> <i>vrf-name</i>                       | VRF name                                                                                                                                                                                                             |
| <b>ip</b> <i>nlb-address</i>                     | NLB address                                                                                                                                                                                                          |
| <b>reflector-port</b><br><i>interface-name</i>   | Reflector port, which serves as a relay port to send the packets to the cluster. For the interface-name, please specify the corresponding interface number and it can be the physical port (the L2AP excluded) only. |
| <b>destination-port</b><br><i>interface-name</i> | Port connecting the cluster with device. For the interface-name, please specify the corresponding interface number and it can be the physical port (the L2AP included) only, but not the SVI or Routed Port.         |

**Defaults** N/A

**Command Mode** Global configuration mode

- Usage Guide**
- The Switch Port and Layer 2 aggregate ports (APs) can be both configured as the cluster connecting port. However, only the Switch Port can be set as the reflector port.
  - After a port has been configured as a reflector port, other configurations are not allowed for this port.
  - Only after configuring the cluster's VRF, IP address and reflector port, the packets are allowed to be routed to the connecting port. If no cluster's connecting port is configured, the packets will flood in the VLAN belonging to the cluster.
  - With the cluster's VRF, IP address and reflector port deleted, the packets routed to the cluster can only be routed to the single server of the cluster.

- When deleting, if no cluster attributes or connecting ports are specified, the entire cluster group will be removed.
- In non-VSU, it is recommended to configure at least 2 Layer-2 AP member ports in different line cards as the reflectors. In VSU, AP member ports had better reside in different line cards on different chassis. Thereby, standby can be configured so that data stream will not be interrupted by port troubles.
- After configuring the cluster attributes, the cluster service is enabled only on the connecting port with cluster configured. If no cluster attribute is configured, the cluster service is not enabled.
- No VRF keyword means the global VRF takes effect.

**Configuration Examples** The following example creates a cluster group and configures the cluster attributes and the cluster connecting port.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# nlb-group 1 vrf vpn-1 ip 192.168.10.1 reflector-port
gigabitEthernet 0/1
Ruijie(config)# nlb-group 1 destination-port gigabitEthernet 0/2, 0/3
```

The following example deletes the cluster attributes of cluster group1.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# no nlb-group 1 vrf vpn-1 ip 192.168.10.1 reflector-port
gigabitEthernet 0/1
```

The following example deletes the connecting port of cluster group1.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# no nlb-group 1 destination-port gigabitEthernet 0/2, 0/3
```

The following example configures the same connecting port for different cluster groups.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#nlb-group 1 ip 192.168.10.10 reflector-port gigabitEthernet
1/1
Ruijie(config)#nlb-group 1 destination-port gigabitEthernet 1/2, 1/3
Ruijie(config)#nlb-group 2 ip 192.168.10.20 reflector-port gigabitEthernet
1/1
Ruijie(config)#nlb-group 2 destination-port gigabitEthernet 1/4, 1/5
```

The following example configures the aggregate port as the reflector port.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-range)#port-group 1
Ruijie(config-if-range)#exit
Ruijie(config)#interface gigabitEthernet 2/1
Ruijie(config-if-range)#port-group 1
Ruijie(config-if-range)#exit
```

```
Ruijie(config)#nlb-group 1 ip 192.168.10.10 reflector-port aggregateport 1
Ruijie(config)#nlb-group 1 destination-port gigabitEthernet 1/2, 1/3
```

**Related  
Commands**

| Command               | Description                         |
|-----------------------|-------------------------------------|
| <b>show nlb-group</b> | Displays the cluster configuration. |

**Platform** N/A**Description**

## 12.2 show nlb-group

Use this command to display the cluster configuration.

**show nlb-group** [ *group\_number* ].

**Parameter  
Description**

| Parameter           | Description          |
|---------------------|----------------------|
| <i>group-number</i> | Cluster group number |

**Defaults** N/A**Command  
Mode** Privileged EXEC mode/Global configuration mode**Usage Guide** N/A**Configuration** The following example displays the cluster configuration.**Examples**

```
Ruijie#show nlb-group 1
group-number: 1
destination-port:
 GigabitEthernet 1/2
 GigabitEthernet 1/3
cluster-vrf: vpn-1
cluster-ip: 192.168.10.10
reflector-port: GigabitEthernet 1/1
```

| Field            | Description                             |
|------------------|-----------------------------------------|
| group-number     | Cluster group number                    |
| destination-port | Port connecting the cluster with device |
| cluster-vrf      | Cluster VRF name                        |
| cluster-ip       | Cluster IP address                      |
| reflector-port   | Reflector port                          |

**Related  
Commands**

| Command          | Description                                                                                                 |
|------------------|-------------------------------------------------------------------------------------------------------------|
| <b>nlb-group</b> | Creates a cluster group and specify the cluster attributes and the port connecting the cluster with device. |

**Platform  
Description**

N/A



## Network Management & Monitoring Commands

---

1. SNMP Commands
2. RMON Commands
3. NTP Commands
4. SNTP Commands
5. SPAN-RSPAN Commands
6. sFlow Commands

# 1 SNMP Commands

## 1.1 no snmp-server

Use this command to disable the SNMP agent function.

**no snmp-server**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** SNMP agent is enabled by default.

**Command mode** Global configuration mode.

**Usage Guide** This command disables the SNMP agent services of all versions supported on the device.

**Configuration Examples** The following example disables the SNMP agent.

```
Ruijie(config)# no snmp-server
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.2 show snmp

Use this command to display the SNMP configuration.

**show snmp [ mib | user | view | group | host | locked-ip | process-mib-time ]**

| Parameter Description | Parameter        | Description                                                   |
|-----------------------|------------------|---------------------------------------------------------------|
|                       | <b>mib</b>       | Displays the SNMP MIBs supported.                             |
|                       | <b>user</b>      | Displays the SNMP user information.                           |
|                       | <b>view</b>      | Displays the SNMP view information.                           |
|                       | <b>group</b>     | Displays the SNMP user group information.                     |
|                       | <b>host</b>      | Displays the explicit host configuration.                     |
|                       | <b>locked-ip</b> | Displays the source IP addresses locked after continuous SNMP |



|                         |                                                              |
|-------------------------|--------------------------------------------------------------|
|                         | authentication failures.                                     |
| <b>process-mib-time</b> | Displays the MIB node requiring the longest processing time. |

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The example below displays the SNMP configuration:

**Examples**

```
Ruijie# show snmp
Chassis: 60FF60
0 SNMP packets input
 0 Bad SNMP version errors
 0 Unknown community name
 0 Illegal operation for community name supplied
 0 Encoding errors
 0 Number of requested variables
 0 Number of altered variables
 0 Get-request PDUs
 0 Get-next PDUs
 0 Set-request PDUs
0 SNMP packets output
 0 Too big errors (Maximum packet size 1472)
 0 No such name errors
 0 Bad values errors
 0 General errors
 0 Response PDUs
 0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
```

|                         |                               |                                            |
|-------------------------|-------------------------------|--------------------------------------------|
| <b>Related Commands</b> | <b>Command</b>                | <b>Description</b>                         |
|                         | <b>snmp-server chassis-id</b> | Specifies the SNMP system sequence number. |

**Platform** N/A

**Description**

### 1.3 snmp trap link-status

Use this command to enable the interface to send link traps. Use the **no** form of this command to

disable the interface to send link traps.

**snmp trap link-status**

**no snmp trap link-status**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP link traps will be sent.

**Command mode** Interface configuration mode

**Usage Guide** This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.

**Configuration** The following example disables the interface to send link traps.

**Examples**

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# no snmp trap link-status
```

The following example enables the interface to send link traps.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.4 snmp-server chassis-id

Use this command to specify the SNMP chassis ID. Use the **no** form of this command to restore the default chassis ID.

**snmp-server chassis-id text**

**no snmp-server chassis-id**

| Parameter   | Parameter   | Description                              |
|-------------|-------------|------------------------------------------|
| Description | <i>text</i> | SNMP chassis ID: numerals or characters. |

**Defaults** The default is 60FF60.

**Command** Global configuration mode.  
**mode**

**Usage Guide** The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the **show snmp** command.

**Configuration** The following example specifies the SNMP chassis ID as 123456:

**Examples** Ruijie(config)# **snmp-server chassis-id 123456**

**Related Commands**

| Command          | Description                      |
|------------------|----------------------------------|
| <b>show snmp</b> | Displays the SNMP configuration. |

**Platform** N/A  
**Description**

## 1.5 snmp-server community

Use this command to specify the SNMP community access string. Use the **no** form of this command to remove the SNMP community access string.

**snmp-server community** [ 0 | 7 ] *string* [ **view** *view-name* ] [ [ **ro** | **rw** ] [ **host** *ipaddr* ] [ **ipv6** *ipv6-aclname* ] [ *aclnum* ] [ *aclname* ]  
**no snmp-server community** [ 0 | 7 ] *string*

**Parameter Description**

| Parameter           | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| 0                   | Indicates that the community string is in plaintext.                                                                      |
| 7                   | Indicates that the community string is in ciphertext.                                                                     |
| <i>string</i>       | Community string, which is the communication password between the NMS and the SNMP agent                                  |
| <i>view-name</i>    | View name                                                                                                                 |
| <b>ro</b>           | Indicates that the NMS can only read the variables of the MIB.                                                            |
| <b>rw</b>           | Indicates that the NMS can read and write the variables of the MIB.                                                       |
| <i>aclnum</i>       | Access list number (1 to 199, and 1300 to 2699), which specifies the IPV4 addresses that are permitted to access the MIB. |
| <i>aclname</i>      | Access list name, which specifies the IPV4 addresses that are permitted to access the MIB.                                |
| <i>ipv6-aclname</i> | IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.                           |
| <i>ipaddr</i>       | Specifies the IP address of the NMS to access the MIB.                                                                    |

**Defaults** All communities are read only by default.

**Command** Global configuration mode.  
**mode**

**Usage Guide** This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB.  
To disable the SNMP agent function, use the **no snmp-server** command.

**Configuration Examples** The following example defines a SNMP community access string named public, which can be read-only.

```
Ruijie(config)# snmp-server community public ro
```

**Related Commands**

| Command            | Description             |
|--------------------|-------------------------|
| <b>access-list</b> | Defines an access list. |

**Platform** N/A  
**Description**

## 1.6 snmp-server contact

Use this command to specify the system contact string. Use the **no** form of this command to remove the system contact string.

**snmp-server contact text**

**no snmp-server contact**

**Parameter Description**

| Parameter   | Description                      |
|-------------|----------------------------------|
| <i>text</i> | Defines a system contact string. |

**Defaults** No system contact string is set by default.

**Command** Global configuration mode.  
**mode**

**Usage Guide** N/A

**Configuration Examples** The following example specifies the SNMP system contract i-net800@i-net.com.cn:

```
Ruijie(config)# snmp-server contact i-net800@i-net.com.cn
```

**Related Commands**

| Command                 | Description                       |
|-------------------------|-----------------------------------|
| <b>show snmp-server</b> | Displays the SNMP configuration.  |
| <b>no snmp-server</b>   | Disables the SNMP agent function. |

**Platform** N/A

## Description

## 1.7 snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap message to NMS. Use the **no** form of this command to disable the SNMP agent to send the SNMP trap message to NMS.

**snmp-server enable traps** [ *notification-type* ]

**no snmp-server enable traps**

Parameter  
Description

| Parameter                | Description                                                                                                                                                                                                                                                                                                                    |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>notification-type</i> | Specifies the type of trap messages.<br>snmp: SNMP trap message<br>bgp: BGP trap message.<br>bridge: Bridge trap message.<br>isis: ISIS trap message.<br>mac-notification: MAC trap message.<br>ospf: OSPF trap message.<br>urpf: uRPF trap message.<br>vrrp: VRRP trap message.<br>web-auth: Web authentication trap message. |

## Defaults

Sending trap message to the NMS is disabled by default.

Command  
mode

Global configuration mode.

## Usage Guide

This command must be used together with the **snmp-server host** command to send the trap message. Specifying no trap type indicates all trap messages are sent.

## Configuration

The following example enables the SNMP agent to send the SNMP trap message.

## Examples

```
Ruijie(config)# snmp-server enable traps snmp
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

Related  
Commands

| Command                 | Description                                            |
|-------------------------|--------------------------------------------------------|
| <b>snmp-server host</b> | Specifies the SNMP host to send the SNMP trap message. |

## Platform

N/A

## Description

## 1.8 snmp-server flow-control

Use this command to configure the SNMP flow control. Use the **no** form of this command to restore the default setting.

**snmp-server flow-control pps** [ *count* ]

**no snmp-server flow-control pps**

| <b>Parameter Description</b>  | Parameter                                                                                 | Description                                                                            |
|-------------------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|                               | <i>count</i>                                                                              | Indicates the number of SNMP requests processed per second, ranging from 50 to 65,535. |
| <b>Defaults</b>               | The default count is 300.                                                                 |                                                                                        |
| <b>Command mode</b>           | Global configuration mode.                                                                |                                                                                        |
| <b>Usage Guide</b>            | N/A                                                                                       |                                                                                        |
| <b>Configuration Examples</b> | The following example configures the number of SNMP requests processed per second to 200. |                                                                                        |
| <b>Examples</b>               | <pre>Ruijie(config)# snmp-server flow-control pps 200</pre>                               |                                                                                        |
| <b>Related Commands</b>       | Command                                                                                   | Description                                                                            |
|                               | N/A                                                                                       | N/A                                                                                    |
| <b>Platform Description</b>   | N/A                                                                                       |                                                                                        |

## 1.9 snmp-server group

Use this command to configure a new SNMP group. Use the **no** form of this command to remove a specified SNMP group.

**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [ **read** *readview* ] [ **write** *writeview* ] [ **access** { [ **ipv6** *ipv6\_aclname* | *aclnum* | *aclname* } }

**no snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

| <b>Parameter Description</b> | Parameter                          | Description                                                                              |
|------------------------------|------------------------------------|------------------------------------------------------------------------------------------|
|                              | <b>v1</b>   <b>v2c</b>   <b>v3</b> | Specifies the SNMP version                                                               |
|                              | <b>auth</b>                        | Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only. |
|                              | <b>noauth</b>                      | Specifies no authentication a packet. This applies to SNMPv3 only.                       |

|                     |                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>priv</b>         | Specifies authentication of a packet with encryption. This applies to SNMPv3 only.                                      |
| <i>readview</i>     | Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.            |
| <i>writeview</i>    | Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent. |
| <i>aclnum</i>       | Access list number, which specifies the IPv4 addresses that are permitted to access the MIB.                            |
| <i>aclname</i>      | Name of the access list, which specifies the IPv4 addresses that are permitted to access the MIB.                       |
| <i>ipv6_aclname</i> | Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.                  |

**Defaults** No SNMP groups are configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures a new SNMP group.

**Examples**

```
Ruijie(config)# snmp-server group mib2user v3 priv read mib2
```

| Related Commands | Command | Description            |
|------------------|---------|------------------------|
|                  |         | <b>show snmp group</b> |

**Platform** N/A

**Description**

## 1.10 snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message. Use the **no** form of this command to remove the specified SNMP host.

**snmp-server host** [ oob ] { *host-addr* | **ipv6** *ipv6-addr* } [ **vrf** *vrfname* ] [ **traps** | **informs** ] [ **version** { 1 | 2c | 3 [ **auth** | **noauth** | **priv** ] ] *community-string* [ **udp-port** *port-num* ] [ **via** *mgmt-name* ] [ *notification-type* ]

**no snmp-server host** [ oob ] { *host-addr* | **ipv6** *ipv6-addr* } [ **vrf** *vrfname* ] [ **traps** | **informs** ] [ **version** { 1 | 2c | 3 { **auth** | **noauth** | **priv** } ] *community-string* [ **udp-port** *port-num* ] [ **via** *mgmt-name* ]

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           |             |

|                             |                                                                                                                                                                                                       |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>oob</b>                  | Indicates the out of band communication, that is, the trap messages are sent to the alarm server through the MGMT port. This option is available only when the device is equipped with the MGMT port. |
| <i>host-addr</i>            | SNMP host address                                                                                                                                                                                     |
| <i>ipv6-addr</i>            | SNMP host address(ipv6)                                                                                                                                                                               |
| <i>vrfname</i>              | Set the name of vrf forwarding table                                                                                                                                                                  |
| <b>trap   informs</b>       | Enables the host to send the SNMP notification as traps or informs.                                                                                                                                   |
| <b>version</b>              | SNMP version: V1, V2C or V3                                                                                                                                                                           |
| <b>auth   noauth   priv</b> | Security level of SNMPv3 users                                                                                                                                                                        |
| <i>community-string</i>     | Community string or username (SNMPv3 version)                                                                                                                                                         |
| <i>port-num</i>             | Port of the SNMP host                                                                                                                                                                                 |
| <b>via mgmt-name</b>        | Specifies the MGMT port.                                                                                                                                                                              |
| <i>notification-type</i>    | The type of the SNMP trap message, such as <b>snmp</b> .<br>If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.                                    |

**Defaults** No SNMP host is specified by default.

**Command mode** Global configuration mode.

**Usage Guide** This command must be used together with the **snmp-server enable traps** command to send the SNMP trap messages to NMS.

Multiple SNMP hosts can be configured to receive the SNMP trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages can be configured.

The **via** parameter can take effect only when the **oob** parameter is configured.

The **vrf** parameter cannot be used together with the **oob** parameter.

**Configuration** The following example specifies an SNMP host to receive the SNMP event trap:

**Examples**

```
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

| <b>Related Commands</b> | Command                         | Description                                           |
|-------------------------|---------------------------------|-------------------------------------------------------|
|                         | <b>snmp-server enable traps</b> | Enables the SNMP agent to send the SNMP trap message. |

**Platform Description** N/A



## 1.11 snmp-server inform

Use this command to configure the resend times for inform requests and the inform request timeout.

Use the **no** form of this command to restore the default settings.

**snmp-server inform** [ *retries* *retry-time* | *timeout* *time* ]

**no snmp-server inform**

| Parameter Description | Parameter        | Description                                                            |
|-----------------------|------------------|------------------------------------------------------------------------|
|                       | <i>retry-num</i> | Specifies the resend times for inform requests, ranging from 0 to 255. |
|                       | <i>time</i>      | Specifies the inform request timeout, ranging from 0 to 21,474,836.    |

**Defaults** The default *retry-num* is 3, and the default **timeout** *time* is 15 seconds.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the resend times of inform requests to 5.

```
Ruijie(config)# snmp-server inform retries 5
```

The following example configures the inform request timeout to 20 seconds.

```
Ruijie(config)# snmp-server inform timeout 20
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.12 snmp-server location

Use this command to set the system location string. Use the **no** form of this command to remove the system location string.

**snmp-server location** *text*

**no snmp-server location**

| Parameter Description | Parameter   | Description                                            |
|-----------------------|-------------|--------------------------------------------------------|
|                       | <i>text</i> | String that describes the system location information. |

**Defaults** No system location string is set by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example sets the system location information:

**Examples** Ruijie(config)# **snmp-server location** start-technology-city 4F of A Buliding

| Related Commands | Command | Description                |
|------------------|---------|----------------------------|
|                  |         | <b>snmp-server contact</b> |

**Platform** N/A  
**Description**

## 1.13 snmp-server logging

Use this command to enable the system to log the GET, GET-NETX and SET operations of NMS.

Use the **no** form of this command to disable the SNMP logging function.

**snmp-server logging { get-operation | set-operation }**

**no snmp-server logging { get-operation | set-operation }**

| Parameter Description | Parameter            | Description                             |
|-----------------------|----------------------|-----------------------------------------|
|                       |                      | <b>get-operation</b>                    |
|                       | <b>set-operation</b> | Logging function for the SET operation. |

**Defaults** The SNMP logging function is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** This command is used to enable the logging function for the GET, GET-NETX and SET operations of NMS.

With the **get-operation** enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID during the GET and GET-NEXT operations.

With the **set-operation** enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID and related values during the SET operation.

A larger number of logs may affect the device performance. Under normal condition, it is recommended to disable the SNMP logging function.

**Configuration** The following example enables the logging function for the GET and SET operations:

**Examples**

```
Ruijie(config)#snmp-server logging get-operation
Ruijie(config)#snmp-server logging set-operation
```

The operation logs are displayed as below:

```
Ruijie#*Feb 7 15:31:16: %SNMP-6-GET_OPER: NMS source-ip(13.12.11.7)
operation(GET) object(id=1.3.6.1.2.1.1.5.0)
```

```
Ruijie#*Feb 7 15:32:16:%SNMP-6-GETN_OPER: NMS source-ip(13.12.11.7)
operation(GET-NEXT) object(id=1.3.6.1.2.1.1.5.0)
```

```
Ruijie#*Feb 7 15:33:23: %SNMP-6-SET_OPER: NMS source-ip(13.12.11.7)
operation(SET) object(id=1.3.6.1.2.1.1.5.0, value=ruijie)
```

The following example disables the logging function for the GET and SET operations:

```
Ruijie(config)#no snmp-server logging get-operation
Ruijie(config)#no snmp-server logging set-operation
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 1.14 snmp-server net-id

Use this command to configure the network element coding information of the device. Use the **no** form of this command to remove the network element coding information.

**snmp-server net-id** *text*

**no snmp-server net-id**

**Parameter Description**

| Parameter   | Description                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>text</i> | Configures the network element coding information of the device. The text length ranges from 1 to 255. The text is case-sensitive, and may contain spaces. |

**Defaults**

No network element coding information is configured by default.

**Command mode**

Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the network element coding text to FZ\_CDMA\_MSC1.

**Examples**

```
Ruijie(config)# snmp-server net-id FZ_CDMA_MSC1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.15 snmp-server packetsize

Use this command to specify the largest size of the SNMP packet. Use the **no** form of this command to restore the default value.

**snmp-server packetsize** *byte-count*

**no snmp-server packetsize**

| Parameter Description | Parameter         | Description |
|-----------------------|-------------------|-------------|
|                       | <i>byte-count</i> |             |

**Defaults** The default is 1,472 bytes.

**Command mode** Global configuration mode.

**Usage Guide** The following example specifies the largest size of SNMP packet as 1,492 bytes:

```
Ruijie(config)# snmp-server packetsize 1492
```

**Configuration** N/A

**Examples**

| Related Commands | Command                         | Description |
|------------------|---------------------------------|-------------|
|                  | <b>snmp-server queue-length</b> |             |

**Platform** N/A

**Description**

## 1.16 snmp-server queue-length

Use this command to specify the length of the message queue for each SNMP trap host. Use the **no** form of this command to restore the default value.

**snmp-server queue-length** *length*

**no snmp-server queue-length**

### Parameter Description

| Parameter     | Description                                |
|---------------|--------------------------------------------|
| <i>length</i> | Queue length. The range is from 1 to 1000. |

### Defaults

The default is 10.

### Command mode

Global configuration mode.

### Usage Guide

Use this command to adjust the length of message queue for each SNMP trap host for the purposes of controlling the speed of sending the SNMP trap messages.

### Configuration

The following example specifies the length of message queue as 100.

### Examples

```
Ruijie(config)# snmp-server queue-length 100
```

### Related Commands

| Command                       | Description                                    |
|-------------------------------|------------------------------------------------|
| <b>snmp-server packetsize</b> | Specifies the largest size of the SNMP packet. |

### Platform

N/A

### Description

## 1.17 snmp-server system-shutdown

Use this command to enable the SNMP message reload function. Use the **no** form of this command to disable the SNMP message reload function.

**snmp-server system-shutdown**

**no snmp-server system-shutdown**

### Parameter Description

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

### Defaults

The SNMP message reload function is disabled by default.

### Command mode

Global configuration mode.

**Usage Guide** Use this command to enable the SNMP message reload function which may enable the system to send the device reload traps to the NMS before the device is reloaded or rebooted.

**Configuration** The following example enables the SNMP message reload function:

**Examples**

```
Ruijie(config)# snmp-server system-shutdown
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.18 snmp-server trap-format private

Use this command to configure the SNMP traps with private fields. Use the **no** form of this command to restore the default trap format.

**snmp-server trap-format private**

**no snmp-server trap-format private**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The private field is not carried in the SNMP trap by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure the SNMP trap format with the private field. Currently, the supported data in the private field is alarm occurrence time. For the specific data type and range of each field, refer to RUIJIE-TRAP-FORMAT-MIB.mib file.

This command does not work if the traps are sent with SNMPv1.

**Configuration** The following example configures the SNMP trap format with the private field.

**Examples**

```
Ruijie(config)# snmp-server trap-format private
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

## Description

## 1.19 snmp-server trap-source

Use this command to specify the source interface of the SNMP trap message. Use the **no** form of this command to restore the default value.

**snmp-server trap-source** *interface*

**no snmp-server trap-source**

### Parameter Description

| Parameter        | Description                                               |
|------------------|-----------------------------------------------------------|
| <i>interface</i> | Specifies the source interface of the SNMP trap messages. |

### Defaults

By default, the IP address of the interface from which the SNMP packet is sent is just the source address.

### Command mode

Global configuration mode.

### Usage Guide

For easy management and identification, you can use this command to fix a local IP address as the SNMP source address.

### Configuration Examples

The following example specifies the IP address of Ethernet interface 0/1 as the source address of the SNMP trap message:

```
Ruijie(config)# snmp-server trap-source fastethernet 0/1
```

### Related Commands

| Command                         | Description                                                    |
|---------------------------------|----------------------------------------------------------------|
| <b>snmp-server enable traps</b> | Enables t the SNMP agent to send the SNMP trap message to NMS. |
| <b>snmp-server host</b>         | Specifies the NMS host to send the SNMP trap message.          |

### Platform

N/A

### Description

## 1.20 snmp-server trap-timeout

Use this command to define the retransmission timeout time of the SNMP trap message. Use the **no** form of this command to restore the default value.

**snmp-server trap-timeout** *seconds*

**no snmp-server trap-timeout**

| Parameter Description | Parameter      | Description                                                                              |
|-----------------------|----------------|------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Timeout ( in seconds) of retransmit the SNMP trap message. The range is from 1 to 1,000. |

**Defaults** The default is 30 seconds.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example specifies the timeout period as 60 seconds.

```
Ruijie(config)# snmp-server trap-timeout 60
```

| Related Commands | Command                         | Description                                                   |
|------------------|---------------------------------|---------------------------------------------------------------|
|                  | <b>snmp-server queue-length</b> | Specifies the length of message queue for the SNMP trap host. |
|                  | <b>snmp-server host</b>         | Specifies the NMS host to send the SNMP trap message.         |
|                  | <b>snmp-server trap-source</b>  | Specifies the source address of the SNMP trap message.        |

**Platform** N/A

**Description**

## 1.21 snmp-server udp-port

Use this command to specify a port to receive SNMP packets. Use the **no** form of this command to restore the default setting.

**snmp-server udp port** *port-number*

**no snmp-server udp port**

| Parameter Description | Parameter          | Description                                   |
|-----------------------|--------------------|-----------------------------------------------|
|                       | <i>port-number</i> | Specifies a port to receive the SNMP packets. |

**Defaults** The default is 161.



**Command** Global configuration mode.  
**mode**

**Usage Guide** N/A

**Configuration** The following example specifies port 15000 to receive the SNMP packets.

**Examples**

```
Ruijie(config)# snmp-server udp-port 15000
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.22 snmp-server user

Use this command to configure a new user to an SNMP group. Use the **no** form of this command to remove a user from an SNMP group.

```
snmp-server user username groupname { v1 | v2c | v3 [encrypted] [auth { md5 | sha } auth-password] [priv des56 priv-password] } [access { [ipv6 ipv6_aclname] [aclnum | aclname] }]]
```

```
no snmp-server user username groupname { v1 | v2c | v3 }
```

**Parameter Description**

| Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>username</i>                    | Name of the user on the host that connects to the agent.                                                                                                                                                                                                                                                                                                             |
| <i>groupname</i>                   | Name of the group to which the user belongs.                                                                                                                                                                                                                                                                                                                         |
| <b>v1</b>   <b>v2c</b>   <b>v3</b> | Specifies the SNMP version. But only SNMPv3 supports the following security parameters.                                                                                                                                                                                                                                                                              |
| <b>encrypted</b>                   | Specifies whether the password appears in cipher text. In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can be used only by the local SNMP engine on the switch. |

|                      |                                                                                                                                                                                                                                           |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auth</b>          | Specifies which authentication level should be used.                                                                                                                                                                                      |
| <i>auth-password</i> | Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.                                                                            |
| <b>priv</b>          | Encryption mode. <i>des56</i> refers to 56-bit DES encryption protocol. <i>priv-password</i> : password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key. |
| <b>md5</b>           | Enables the MD5 authentication protocol. While the <b>sha</b> enables the SHA authentication protocol.                                                                                                                                    |
| <i>aclnumber</i>     | Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.                                                                                                                                              |
| <i>aclname</i>       | Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.                                                                                                                                         |
| <i>ipv6_aclname</i>  | Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.                                                                                                                                    |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

```
Ruijie(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv
des56 despassstr
```

| Related Commands | Command | Description           |
|------------------|---------|-----------------------|
|                  |         | <b>show snmp user</b> |

**Platform** N/A

**Description**

## 1.23 snmp-server view

Use this command to configure an SNMP view. Use the **no** form of this command to remove an SNMP view.

**snmp-server view** *view-name oid-tree* { **include** | **exclude** }

**no snmp-server view** *view-name* [ *oid-tree* ]

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |                                                         |                                                       |
|--------------------|---------------------------------------------------------|-------------------------------------------------------|
| <b>Description</b> |                                                         |                                                       |
|                    | <i>view-name</i>                                        | View name                                             |
|                    | <i>oid-tree</i>                                         | Specifies the MIB object to associate with the view.  |
|                    | <b>include</b>                                          | Includes the sub trees of the MIB object in the view. |
| <b>exclude</b>     | Excludes the sub trees of the MIB object from the view. |                                                       |

**Defaults** By default, a view is set to access all MIB objects.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

**Examples** Ruijie(config)# snmp-server view mib2 1.3.6.1 include

| <b>Related Commands</b> | Command               | Description                           |
|-------------------------|-----------------------|---------------------------------------|
|                         | <b>show snmp view</b> | Displays the SNMP view configuration. |

**Platform** N/A

**Description**

## 2 RMON Commands

### 2.1 rmon alarm

Use this command to monitor a MIB variable. Use the **no** form of this command to remove the alarm entry.

**rmon alarm** *number variable interval {absolute | delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner ownername]*  
**no rmon alarm** *number*

| Parameter   | Parameter                      | Description                                                                                                                                                                                                      |
|-------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description | <i>number</i>                  | Alarm number. The value ranges from 1-65,535.                                                                                                                                                                    |
|             | <i>variable</i>                | Alarm variable. The value is a character string consisting of 1 to 255 characters in OID dotted format (the format is entry.integer.instance or a leaf node named .instance, for example. 1.3.6.1.2.1.2.1.10.1). |
|             | <i>interval</i>                | Sampling interval. The value ranges from 1 to 2,147,483,647 in the unit of second.                                                                                                                               |
|             | <b>absolute</b>                | Absolute sampling. In this mode, when the sampling time arrives, the system directly invokes the variable value.                                                                                                 |
|             | <b>delta</b>                   | Delta sampling. In this mode, when the sampling time arrives, the system invokes the delta value of the variable within the sampling interval.                                                                   |
|             | <b>rising-threshold value</b>  | Rising threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647.                                                                   |
|             | <i>event-number</i>            | The event number ranges from 1 to 65,535.                                                                                                                                                                        |
|             | <b>falling-threshold value</b> | Falling threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647                                                                   |
|             | <b>owner ownername</b>         | Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.                                                                                                     |

**Default** N/A.

**Command mode** Global configuration mode.

**Usage guidelines** The RGOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.

**Examples** The example below monitors the MIB variable instance ifInNUcastPkts.6.

```
Ruijie(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta
```

```
rising-threshold 20 1 falling-threshold 10 1 owner zhangsan
```

**Related commands**

| Command                                                                                                                                                  | Description               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| <b>rmon event</b> <i>number</i> [ <b>log</b> ] [ <b>trap</b> <i>community</i> ]<br><b>description</b> <i>string</i> [ <b>owner</b> <i>owner-string</i> ] | Adds an event definition. |

## 2.2 rmon collection history

Use this command to enable history statistics on the Ethernet interface. Use the **no** form of this command to remove the history entry.

**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

**no rmon collection history** *index*

**Parameter description**

| Parameter                              | Description                                                                                                                               |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <i>index</i>                           | Index of a history entry. The value ranges from 1 to 65,535.                                                                              |
| <b>owner</b><br><i>ownername</i>       | Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.                              |
| <b>buckets</b><br><i>bucket-number</i> | Capacity of a history entry (that is, the maximum number of history entries). The value ranges from 1 to 65,535. The default value is 10. |
| <b>interval</b><br><i>seconds</i>      | Statistics period. The unit is second. The value ranges from 1 to 3,600. The default value is 1,800 seconds.                              |

**Default** N/A.

**Command mode** Interface configuration mode.

**Usage guidelines** The configured history control entry parameters cannot be modified. And the history entry can be removed from the interface where the entry configured.

The example below enables log statistics on interface GigabitEthernet 0/1.

**Examples**

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet0/1)#rmon history 1 owner UserA buckets 5
interval 60
```

**Related commands**

| Command                                                                         | Description                                         |
|---------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>rmon collection stats</b> <i>index</i><br>[ <b>owner</b> <i>owner-name</i> ] | Adds a statistical entry on the Ethernet interface. |

## 2.3 rmon collection stats

Use this command to monitor an Ethernet interface. Use the **no** form of this command to remove the configuration.

**rmon collection stats** *index* [**owner** *owner-string*]

**no rmon collection stats** *index*

| Parameter description | Parameter                     | Description                                                                                                                            |
|-----------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>index</i>                  | Index of the statistic table. The value ranges from 1 to 65,535.                                                                       |
|                       | <b>owner</b> <i>ownername</i> | Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive and do not contain spaces. |

**Default** N/A.

**Command mode** Interface configuration mode.

**Usage guidelines** N/A.

The example below enables monitoring the statistics of interface GigabitEthernet 0/1.

### Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet0/1)# rmon stats 1 owner UserA
```

| Related commands | Command                                                                                                                                                      | Description                   |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
|                  | <b>rmon collection history</b> <i>index</i> [ <b>owner</b> <i>owner-name</i> ]<br>[ <b>buckets</b> <i>bucket-number</i> ] [ <b>interval</b> <i>seconds</i> ] | Adds a history control entry. |

## 2.4 rmon event

Use this command to define an event. Use the **no** form of this command to remove the event entry.

**rmon event** *number* [**log**] [**trap** *community*] [*description-string*] [**description**

*description-string*] [**owner** *owner-name*]

**no rmon event** *number*

| Parameter description | Parameter                    | Description                                                                                                    |
|-----------------------|------------------------------|----------------------------------------------------------------------------------------------------------------|
|                       | <i>number</i>                | Event number. The value ranges from 1 to 65,535.                                                               |
|                       | <b>log</b>                   | (Optional) Log event. When a log event is triggered, the system records a log.                                 |
|                       | <b>trap</b> <i>community</i> | (Optional) Trap event. When a trap event is triggered, the system sends trap with the group named "community". |

|                                                 |                                                                                                                         |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>description</b><br><i>description-string</i> | (Optional) Description of the event. The value is a character string consisting of 1 to 127 characters.                 |
| <b>owner</b><br><i>owner-name</i>               | (Optional) Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive. |

**Default** N/A.

**Command mode** Global configuration mode.

**Usage guidelines** N/A.

**Examples**

The example below defines the event actions: log event and send trap message.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#rmon event 1 log trap public description "ifInNUcastPkts
is abnormal" owner UserA
```

| Command                                                                                                                                                              | Description          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>rmon alarm</b> <i>number variable interval {absolute   delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner ownername]</i> | Adds an alarm entry. |

## 2.5 show rmon

**Default** Use this command to display the RMON configuration.  
**show rmon**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

**Examples**

The example below displays the RMON configuration.

```
Ruijie#show rmon
ether statistic table:
 index = 1
 interface = GigabitEthernet 0/1
 owner = admin
 status = 0
 dropEvents = 61
 octets = 170647461
```

```
pkts = 580375
broadcastPkts = 2135
multiPkts = 3615
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 3254668
packets65To127Octets = 1833370
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865
```

rmon history control table:

```
index = 1
interface = GigabitEthernet 0/1
bucketsRequested = 5
bucketsGranted = 5
interval = 60
owner = UserA
stats = 1
```

rmon history table:

```
index = 1
sampleIndex = 2485
intervalStart = 7d:22h:56m:38s
dropEvents = 0
octets = 5840
pkts = 27
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0
```

rmon alarm table:

```
index: 1
interval: 60
```



```

oid = 1.3.6.1.2.1.2.2.1.12.6
sampleType: 2
alarmValue: 0
startupAlarm: 3
risingThreshold: 20
fallingThreshold: 10
risingEventIndex: 1
fallingEventIndex: 1
owner: UserA
status: 1

rmon event table:
 index = 1
 description = ifInNUcastPkts is abnormal
 type = 4
 community = public
 lastTimeSent = 0d:0h:0m:0s
 owner =UserA
 status = 1

rmon log table:
 eventIndex = 1
 index = 1
 logTime = 6 d:19 h:21 m:48 s
 logDescription = ifInNUcastPkts is abnormal

```

**Related commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

## 2.6 show rmon alarm

**Default** Use this command to display the RMON alarm table.

**show rmon alarm**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the RMON alarm table.

**Examples**

```

Ruijie#show rmon alarm
rmon alarm table:

```

```

index: 1
interval: 60
oid = 1.3.6.1.2.1.2.2.1.12.6
sampleType: 2
alarmValue: 0
startupAlarm: 3
risingThreshold: 20
fallingThreshold: 10
risingEventIndex: 1
fallingEventIndex: 1
owner: UserA
status: 1

```

**Related commands**

| Command                                                                                                                                                                                                                                              | Description          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>rmon alarm</b> <i>number variable</i><br><i>interval {absolute   delta }</i><br><b>rising-threshold</b> <i>value</i><br><i>[event-number]</i> <b>falling-threshold</b> <i>value</i><br><i>[event-number]</i> [ <b>owner</b><br><i>ownername</i> ] | Adds an alarm entry. |

## 2.7 show rmon event

Use this command to display the event configuration.

**show rmon event**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the event configuration.

**Examples**

```

Ruijie#show rmon event
rmon event table:
 index = 1
 description = ifInNUcastPkts is abnormal
 type = 4
 community = public
 lastTimeSent = 0d:0h:0m:0s
 owner =UserA
 status = 1

```

```
rmon log table:
 eventIndex = 1
 index = 1
 logTime = 6d:19h:21m:48s
 logDescription = ifInNUcastPkts is abnormal
```

**Related  
commands**

| Command                                                                                                                                                            | Description          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>rmon event</b> <i>number</i> [ <b>log</b> ] [ <b>trap</b> <i>community</i> ] [ <b>description</b> <i>description-string</i> ] [ <b>owner</b> <i>ownername</i> ] | Adds an event entry. |

## 2.8 show rmon history

Use this command to display the history information.

**show rmon history**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the history information.

```
Ruijie#show rmon history
rmon history control table:
 index = 1
 interface = GigabitEthernet 0/1
 bucketsRequested = 5
 bucketsGranted = 5
 interval = 60
 owner = UserA
 stats = 1
```

**Examples**

```
rmon history table:
 index = 1
 sampleIndex = 2485
 intervalStart = 7d:22h:56m:38s
 dropEvents = 0
 octets = 5840
 pkts = 27
 broadcastPkts = 0
 multiPkts = 0
 crcAlignErrors = 0
 underSizePkts = 0
```

```

overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

```

**Related commands**

| Command                                                                                                                                                   | Description                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <b>rmon collection history</b> <i>index</i><br>[owner <i>ownername</i> ] [ <b>buckets</b><br><i>bucket-number</i> ] [ <b>interval</b><br><i>seconds</i> ] | Adds a history control entry. |

## 2.9 show rmon statistics

Use this command to display the RMON statistics.

**show rmon statistics**

**Default**

N/A.

**Command mode**

Privileged EXEC mode.

**Usage guidelines**

The example below displays the RMON statistics.

**Examples**

```

Ruijie#show rmon statistics
ether statistic table:
 index = 1
 interface = GigabitEthernet 0/1
 owner = admin
 status = 0
 dropEvents = 61
 octets = 170647461
 pkts = 580375
 broadcastPkts = 2135
 multiPkts = 3615
 crcAlignErrors = 0
 underSizePkts = 0
 overSizePkts = 0
 fragments = 0
 jabbers = 0
 collisions = 0
 packets64Octets = 3254668
 packets65To127Octets = 1833370

```

```
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865
```

**Related  
commands**

| Command                                                                        | Description               |
|--------------------------------------------------------------------------------|---------------------------|
| <b>rmon collection stats</b> <i>index</i> [ <b>owner</b> <i>owner-string</i> ] | Adds a statistical entry. |

## 3 NTP Commands

### 3.1 no ntp

Use this command to disable Network Time Protocol (NTP), and clear all NTP configuration.

**no ntp**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** NTP is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** By default, NTP is disabled. However, once the NTP server or the NTP authentication is configured, the NTP service will be enabled.

**Configuration** The following example disables NTP.

**Examples** Ruijie(config)#**no ntp**

| Related Commands | Command           | Description              |
|------------------|-------------------|--------------------------|
|                  | <b>ntp server</b> | Specifies an NTP server. |

**Platform** N/A

**Description**

### 3.2 ntp access-group

Use this command to configure an access group to control NTP access. Use the **no** form of this command to remove the peer access group.

**ntp access-group** { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*

**no ntp access-group** { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* |

*access-list-name*

| Parameter Description | Parameter   | Description                                                                                                                           |
|-----------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>peer</b> | Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list. |

|                           |                                                                                                                                                                          |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>serve</b>              | Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers. |
| <b>serve-only</b>         | Allows the device to receive only time requests from the servers specified in the access list.                                                                           |
| <b>query-only</b>         | Allows the device to receive only NTP control queries from servers specified in the access list.                                                                         |
| <i>access-list-number</i> | Access control list number, ranging from 1 to 99 and 1300 to 1999.                                                                                                       |
| <i>access-list-name</i>   | Access control list name.                                                                                                                                                |


**Defaults** No access rule to control NTP access is configured by default, namely, NTP access is granted to all devices.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure an access group to control NTP access, providing a minimal security measures (more secure way is to use the NTP authentication mechanism).

The NTP service enables the access group options to be scanned in the following order, from least restrictive to most restrictive: **peer**, **serve**, **serve-only**, **query-only**.

If you do not configure any access groups, NTP access is granted to all devices. However, once you configure the access rule, NTP access is granted only to the devices specified in the access list.

 NTP control query is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

**Configuration Examples** The following example shows how to allow the device to only receive time requests from the device of 192.168.1.1.

```
Ruijie(config)# access-list 1 permit 192.168.1.1
Ruijie(config)# ntp access-group serve-only 1
```

**Related Commands**

| Command               | Description                        |
|-----------------------|------------------------------------|
| <b>ip access-list</b> | Creates an IP access control list. |

**Platform** N/A

**Description**

### 3.3 ntp authenticate

Use this command to enable NTP authentication. Use the **no** form of this command to disable NTP

authentication.

**ntp authenticate**

**no ntp authenticate**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** Disabled.

**Command mode** Global configuration mode.

**Usage Guide** If NTP authentication is disabled, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the NTP authentication and configure other keys globally.

NTP authentication is implemented through the trusted key specified by the **ntp authentication-key** and **ntp trusted-key** commands.

**Configuration Examples** After an authentication key is configured and specified as the global trusted key, enable NTP authentication.

```
Ruijie(config)#ntp authentication-key 6 md5 woooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp authenticate
```

| Related Commands | Command                       | Description                         |
|------------------|-------------------------------|-------------------------------------|
|                  | <b>ntp authentication-key</b> | Sets the global authentication key. |
|                  | <b>ntp trusted-key</b>        | Configures the global trusted key.  |

**Platform Description** N/A

### 3.4 ntp authentication-key

Use this command to configure an NTP authentication key. Use the **no** form of this command to remove the NTP authentication key.

**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]

**no ntp authentication-key** *key-id*

| Parameter Description | Parameter         | Description                           |
|-----------------------|-------------------|---------------------------------------|
|                       | <i>key-id</i>     | Key ID, ranging from 1 to 4294967295. |
|                       | <i>key-string</i> | Key string                            |



|                 |                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>enc-type</i> | (Optional) Whether this key is encrypted, where, 0 indicates the key is not encrypted, 7 indicates the key is encrypted simply. The key is not encrypted by default. |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Defaults** NTP authentication key is not configured by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure an NTP authentication key and enables the **md5** algorithm for authentication. Each key presents a unique key ID, which can be configured as a trusted key using the **ntp trusted-key** command..  
You can configure up to 1024 NTP authentication keys. However, each server can support only one key.

**Configuration** The following example configures an NTP authentication key.

**Examples**

```
Ruijie(config)#ntp authentication-key 6 md5 woooooop
```

| Related Commands       | Command                        | Description                 |
|------------------------|--------------------------------|-----------------------------|
|                        | <b>ntp authenticate</b>        | Enables NTP authentication. |
| <b>ntp trusted-key</b> | Configures an NTP trusted key. |                             |
| <b>ntp server</b>      | Specifies an NTP server.       |                             |

**Platform** N/A

**Description**

### 3.5 ntp disable

Use this command to disable the device to receive NTP packets on the specified interface.

**ntp disable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** All NTP packets can be received by default.

**Command mode** Interface configuration mode.

**Usage Guide** The NTP message received on any interface can be provided to the client to carry out the clock adjustment. The function can be set to shield the NTP message received from the corresponding interface.

By default, the device receives NTP packets on all interfaces, and adjust clock for the client. You can use this command to disable the device to receive NTP packets on the specified interface.

 This command is configured only the interface that can receive and send IP packets.

**Configuration** The following example disables the device to receive the NTP packets.

**Examples** Ruijie(config-if)# no ntp disable

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

### 3.6 ntp master

Use this command to configure the device to act as an authoritative NTP server, synchronizing time to other devices. Use the **no** form of this command to remove the device as an authoritative NTP server.

**ntp master** [ *stratum* ]

**no ntp master**


**Parameter  
Description**


| Parameter      | Description                                                 |
|----------------|-------------------------------------------------------------|
| <i>stratum</i> | Stratum level. The range is from 1 to 15. The default is 8. |

**Defaults** N/A

**Command  
mode** Global configuration mode.

**Usage Guide** In general, the local device synchronizes time from the external time source directly or indirectly. However, if the time synchronization fails due to network connection trouble, you can use this command to configure the local device to act as an authoritative NTP server to synchronize time to other devices. Once configured, the device will not perform time synchronization with the time source which is of a higher stratum.

 Configuring the device to act as an authoritative NTP server (in particular, specify a lower stratum level), may be likely to overwrite the effective time. If multiple devices in the same network are configured with this command, the time synchronization may be instable due to the time difference between the devices.

 Before configuring this command, you need to manually correct the system clock to avoid too much bias if the device has never performed time synchronization with the external clock

source.

**Configuration** The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12:

**Examples**

```
Ruijie(config)# ntp master 12
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

### 3.7 ntp server

Use this command to specify a NTP server for the NTP client. Use the **no** form of this command to delete the specified NTP server.

```
ntp server [oob | vrf vrf-name] { ip-addr | domain | ip domain | ipv6 domain } [version version]
[source if-name] [key keyid] [prefer] [via mgmt-name]
```

```
no ntp server ip-addr
```

**Parameter Description**

| Parameter           | Description                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>oob</b>          | (Optional) Accesses the NTP server from the MGMT interface. By default, this option is disabled.                                               |
| <b>vrf vrf-name</b> | Specifies the virtual routing and forwarding (VRF) name. By default, this parameter is disabled.                                               |
| <i>ip-addr</i>      | Sets the IP address of the NTP server. The address can be in IPv4 or IPv6 format.                                                              |
| <i>domain</i>       | Sets the domain name of the NTP server, supporting IPv4 and IPv6.                                                                              |
| <i>version</i>      | (Optional) Specifies the NTP version (1-3). The default is NTPv3.                                                                              |
| <i>if-name</i>      | (Optional) Specifies the source interface from which the NTP message is sent (L3 interface).                                                   |
| <i>keyid</i>        | (Optional) Specifies the encryption key adopted when communication with the corresponding server. The key ID range is from 1 to 4,294,967,295. |
| <b>prefer</b>       | (Optional) Specifies the given NTP server as the preferred one.                                                                                |
| <i>mgmt-name</i>    | (Optional) Specifies the egress MGMT interface for the packets in oob mode.                                                                    |

**Defaults** No NTP server is configured by default.

**Command** Global configuration mode.

**mode**

**Usage Guide** At present, RGOS system only supports clients other than servers. Up to 20 servers can be synchronized.

To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server.

In the same condition (for instance, precision), the prefer clock is used for synchronization.

 The source interface of NTP packets must be configured with the IP address and can be communicated with the peer.

**Configuration** The following example configures an NTP server.

**Examples** For IPv4: `Ruijie(config)# ntp server 192.168.210.222`

For IPv6: `Ruijie(config)# ntp server 10::2`

**Related Commands**

| Command             | Description   |
|---------------------|---------------|
| <code>no ntp</code> | Disables NTP. |

**Platform** N/A

**Description**

### 3.8 ntp trusted-key

Use this command to set a global trusted key. Use the **no** form of this command to remove the global trusted key.

**ntp trusted-key** *key-id*

**no ntp trusted-key** *key-id*

**Parameter Description**

| Parameter     | Description                                          |
|---------------|------------------------------------------------------|
| <i>key-id</i> | Global trusted key ID, ranging from 1 to 4294967295. |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

**Configuration** The following example configures an authentication key and sets it as a trusted key.

**Examples**

```
Ruijie(config)#ntp authentication-key 6 md5 woooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp server 192.168.210.222 key 6
```

**Related  
Commands**

| Command                       | Description                           |
|-------------------------------|---------------------------------------|
| <b>ntp authenticate</b>       | Enables NTP authentication.           |
| <b>ntp authentication-key</b> | Configures an NTP authentication key. |
| <b>ntp server</b>             | Configures an NTP server.             |

**Platform**

N/A

**Description**

### 3.9 ntp update-calendar

Use this command to enable the NTP client to periodically update the device clock with the time synchronized from the external source clock. Use the **no** form of this command to remove this function.

**ntp update-calendar**

**no ntp update-calendar**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

By default, update the calendar periodically is not configured.

**Command  
mode**

Global configuration mode.

**Usage Guide**

By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

**Configuration** The following example configures the NTP update calendar periodically.

**Examples**

```
Ruijie(config)# ntp update-calendar
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

### 3.10 show ntp server

Use this command to display the NTP server configuration.

**show ntp server**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the NTP server.

**Examples**

```
Ruijie# show ntp server
ntp-server source keyid prefer version

10::2 None None FALSE 3
192.168.210.222 None None FALSE 3
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

### 3.11 show ntp status

Use this command to display the NTP configuration.

**show ntp status**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

**Usage Guide** Use this command to display the NTP configuration. No configuration is displayed before the synchronization server is configured for the first time.

**Configuration** The following example displays the NTP configuration.

**Examples**

```
Ruijie# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D4BD819B.433892EE (01:27:55.000 UTC)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 4 SNTP Commands

### 4.1 show sntp

Use this command to display the SNTP configuration.

**show sntp**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

**Command  
mode**

Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example displays the SNTP configuration.

**Examples**

```
Ruijie# show sntp
SNTP state : Enable
SNTP server : 192.168.4.12
SNTP sync interval : 60
Time zone : +8
```

**Related  
Commands**

| Command            | Description   |
|--------------------|---------------|
| <b>sntp enable</b> | Enables SNTP. |

**Platform  
Description**

N/A

### 4.2 sntp enable

Use this command to enable the SNTP function. Use the **no** form of this command to restore the default value.

**sntp enable**

**no sntp enable**

**Parameter**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|



|                               |                                               |                                  |
|-------------------------------|-----------------------------------------------|----------------------------------|
| <b>Description</b>            |                                               |                                  |
|                               | N/A                                           | N/A                              |
| <b>Defaults</b>               | SNTP is disabled by default.                  |                                  |
| <b>Command mode</b>           | Global configuration mode.                    |                                  |
| <b>Usage Guide</b>            | N/A                                           |                                  |
| <b>Configuration Examples</b> | The following example enables SNTP.           |                                  |
|                               | <pre>Ruijie(config)# <b>sntp enable</b></pre> |                                  |
| <b>Related Commands</b>       | <b>Command</b>                                | <b>Description</b>               |
|                               | <b>show sntp</b>                              | Displays the SNTP configuration. |
| <b>Platform Description</b>   | N/A                                           |                                  |

### 4.3 sntp interval

Use this command to set the interval for the SNTP client to synchronize its clock with the NTP/SNTP server. Use the **no** form of this command to restore the default synchronization interval.

**sntp interval** *seconds*

**no sntp interval**

|                               |                                                                                                   |                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                                                  | <b>Description</b>                                                                |
|                               | <i>seconds</i>                                                                                    | Synchronization interval. The unit is second, and the range is from 60 to 65,535. |
| <b>Defaults</b>               | The default synchronization interval is 1,800 seconds.                                            |                                                                                   |
| <b>Command mode</b>           | Global configuration mode.                                                                        |                                                                                   |
| <b>Usage Guide</b>            | To make the synchronization interval configuration effective, run the <b>sntp enable</b> command. |                                                                                   |
| <b>Configuration Examples</b> | The following example configures the synchronization interval to 3,600 seconds.                   |                                                                                   |
|                               | <pre>Ruijie(config)# sntp interval 3600</pre>                                                     |                                                                                   |
| <b>Related Commands</b>       | <b>Command</b>                                                                                    | <b>Description</b>                                                                |
|                               |                                                                                                   |                                                                                   |

|                    |                                  |
|--------------------|----------------------------------|
| <b>sntp enable</b> | Enables SNTP.                    |
| <b>show sntp</b>   | Displays the SNTP configuration. |

**Platform** N/A

**Description**

## 4.4 sntp server

Use this command to specify an SNTP server. Use the **no** form of this command to remove the SNTP server.

**sntp server** [ **oob** ] { *ip-address* | *domain* } [ **via** *mgmt-name* ] [ **source** *source-ip-address* ]  
**no sntp server**

**Parameter Description**

| Parameter                | Description                                                                 |
|--------------------------|-----------------------------------------------------------------------------|
| <i>ip-address</i>        | IP address of the SNTP server.                                              |
| <b>oob</b>               | (Optional) Accesses the SNTP server from the MGMT interface.                |
| <i>domain</i>            | Specifies the domain name of the SNTP server.                               |
| <i>source-ip-address</i> | (Optional) Indicates the specified source IP address.                       |
| <i>mgmt-name</i>         | (Optional) Specifies the egress MGMT interface for the packets in oob mode. |

**Defaults** No SNTP server is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** As SNTP is fully compatible with NTP, the SNTP server can be used as an NTP server in Internet.

**Configuration** The following example specifies an SNTP server in Internet.

**Examples**

```
Ruijie(config)# sntp server 192.168.4.12
```

**Related Commands**

| Command            | Description                      |
|--------------------|----------------------------------|
| <b>show sntp</b>   | Displays the SNTP configuration. |
| <b>sntp enable</b> | Enables SNTP.                    |

**Platform** N/A

**Description**

## 5 SPAN-RSPAN Commands

### 5.1 mac-loopback

Use this command to enable MAC loopback. Use the **no** form of this command to disable MAC loopback.

**mac-loopback**

**no mac-loopback**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** MAC loopback is disabled by default.

**Command mode** Interface configuration mode.

**Usage Guide** The MAC loopback feature must be enabled on the interfaces for purposes of local one-to-many mirroring. (Please enable the MAC loopback feature on the down interface, and do not add other configurations to the interface.)

**Configuration Examples** The following example configures a remote VLAN.

```
Ruijie(config)#vlan 100
Ruijie(config-vlan)#remote-span
Ruijie(config-vlan)#exit
```

The following example configures a session and specifies the mirrored port.

```
Ruijie(config)#monitor session 1 remote-source
Ruijie(config)#monitor session 1 source interface gigabitEthernet 4/1 both
```

The following example configures the mirroring port, and enables MAC loopback on the port.

```
Ruijie(config)#monitor session 1 destination remote vlan 100 interface
gigabitEthernet 4/2 switch
Ruijie(config)#interface gigabitEthernet 4/2
Ruijie(config-if-GigabitEthernet 4/2)#switchport access vlan 100
Ruijie(config-if-GigabitEthernet 4/2)#mac-loopback
```

The following example adds interfaces GigabitEthernet 4/3-4 to the remote VLAN.

```
Ruijie(config)#interface range gigabitEthernet 4/3-4
Ruijie(config-if-range)#switchport access vlan 100
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 5.2 monitor session

Use this command to configure the SPAN session and specify the source port (monitored port).

**monitor session** *session-num* **source interface** *interface-id* [ **both** | **rx** | **tx** ]

Use this command to configure the SPAN session mirroring only the traffic permitted by the access list

**monitor session** *session-num* **source interface** *interface-id* **rx acl** *acl-name*

Use this command to configure the SPAN session and specify the destination port (monitoring port).

**monitor session** *session-num* **destination interface** *interface-id* [**switch** ]

Use this command to configure the remote SPAN session ID on the source device..

**monitor session** *session-num* **remote-source**

Use this command to configure the remote SPAN session ID on the destination device.

**monitor session** *session-num* **remote-destination**

Use this command to configure the remote SPAN session and specify the remote SPAN destination VLAN.

**monitor session** *session-num* **destination remote vlan** *remote-vlan-id* **interface** *interface-id*  
[ **switch** ]

Use this command to configure the SPAN session and specify the source VLAN to monitor. Note that the source VLAN should not be a remote VLAN.

**monitor session** *session-num* **source vlan** *vlan-id* [ **rx** | **tx** | **both** ]

Use this command to limit the SPAN source traffic to specific VLANs.

**monitor session** *session-num* **filter vlan** *vlan-id-list* [ **rx** | **tx** | **both** ]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the specified SPAN session.

**no monitor session** *session-num* [ **source interface** *interface-id* | **destination interface** *interface-id* ]

Use this command to remove the specified remote SPAN session, or remove the destination port of the remote SPAN session.

**no monitor session** *session-num* [ **destination remote vlan** *remote-vlan-id* **interface** *interface-id* ]

Use this command to remove the specified remote SPAN session, or remove the destination port of the remote SPAN session.

**default monitor session** *session-num* [ **destination remote vlan** *remote-vlan-id* **interface** *interface-id* ]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the SPAN session.

**default monitor session** *session-num* { **source interface** *interface-id* | **destination interface** *interface-id* }

**Parameter  
Description**

| Parameter                  | Description                                                                           |
|----------------------------|---------------------------------------------------------------------------------------|
| <i>session_number</i>      | SPAN session number                                                                   |
| <i>interface-id</i>        | Interface name                                                                        |
| <b>acl</b> <i>acl-name</i> | Access list name                                                                      |
| <i>remote-vlan-id</i>      | Remote VLAN ID                                                                        |
| <i>vlan-id</i>             | VLAN ID (remote VLAN excluded)                                                        |
| <i>vlan-id-list</i>        | VLAN list (remote VLAN excluded)                                                      |
| <b>rx</b>                  | Monitors the only received traffic.                                                   |
| <b>tx</b>                  | Monitors the only transmitted traffic.                                                |
| <b>both</b>                | Monitors both received and transmitted traffic. This is the default.                  |
| <b>switch</b>              | Enables switching on the destination port. Switching function is disabled by default. |

**Defaults** Port monitoring is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure SPAN or remote SPAN, and specify the source port or destination port.  
If the **both**, **rx** or **tx** is not specified for the source port, the **both** parameter is the default.  
Configuring an access list for the source port indicates that only the traffic permitted by the access list is monitored.  
The **switch** feature is disabled on the destination port.

**Configuration** The following example configures the source port and destination port of the SPAN session.

**Examples**

```
Ruijie(config)# monitor session 1 source interface gigabitEthernet 0/1
Ruijie(config)# monitor session 1 destination interface gigabitEthernet 0/2
```

The following example configures the SPAN session mirroring only the traffic permitted by the access list.

```
Ruijie(config)# monitor session 3 source interface gigabitEthernet 0/3 rx acl
90
```

The following example configures a remote SPAN session.

```
Ruijie(config)# monitor session 10 remote-source
```

The following example configures the destination port of the remote SPAN session.

```
Ruijie(config)# monitor session 4 destination remote vlan 10 interface
gigabitEthernet 0/5
```

The following example configures the source VLAN of the SPAN session.

```
Ruijie(config)# monitor session 1 source vlan 1
```

The following example removes the SPAN session.

```
Ruijie(config)# no monitor session 1
```

The following example removes the source port and destination port of the SPAN session.

```
Ruijie(config)# no monitor session 1 source interface gigabitEthernet 0/18
Ruijie(config)# no monitor session 1 destination interface gigabitEthernet
0/18
```

#### Related Commands

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

#### Platform Description

N/A

## 5.3 remote-span

Use this command to configure a remote SPAN VLAN in VLAN configuration mode. Use the **no** form of this command to disable the remote SPAN VLAN.

**remote-span**

**no remote-span**

#### Parameter Description

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** Remote SPAN VLAN is disabled by default.

**Command mode** VLAN configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures a remote SPAN VLAN.

**Examples**

```
Ruijie(config)# vlan 100
Ruijie(config-vlan)# remote-span
```

| Related Commands | Command | Description      |
|------------------|---------|------------------|
|                  |         | <b>show vlan</b> |

**Platform** N/A

**Description**

## 5.4 show monitor

Use this command to display the SPAN configurations.

**show monitor** [ **session** *session\_number* ]

| Parameter Description | Parameter | Description           |
|-----------------------|-----------|-----------------------|
|                       |           | <i>session_number</i> |

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode and interface configuration mode

**Usage Guide** N/A

**Configuration** This following example displays all SPAN sessions.

**Examples**

```
Ruijie(config)# show monitor
sess-num: 2
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/5 frame-type Both
dest-intf:
TenGigabitEthernet 0/6
sess-num: 1
span-type: LOCAL_SPAN
```

```
src-intf:
TenGigabitEthernet 0/3 frame-type Both
dest-intf:
```

The following example displays SPAN session 1.

```
Ruijie(config)# show monitor session 1
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/3 frame-type Both
dest-intf:
TenGigabitEthernet 0/4
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A



## 6 sFlow Commands

### 6.1 sflow agent

Use this command to configure the address of the sFlow Agent.

```
sflow agent { address { ip-address | ipv6 ipv6-address } } | { interface { interface-name | ipv6 interface-name } }
```

Use this command to delete the address of the sFlow Agent.

```
no sflow agent { address | interface }
```

Use this command to restore the default setting.

```
default sflow agent { address | interface }
```

#### Parameter Description

| Parameter                         | Description                                   |
|-----------------------------------|-----------------------------------------------|
| <b>address</b>                    | Configures the IP address of the sFlow Agent. |
| <i>ip-address</i>                 | sFlow Agent IPv4 address.                     |
| <b>ipv6</b> <i>ipv6-address</i>   | sFlow Agent IPv6 address.                     |
| <b>interface</b>                  | Configures the interface of the sFlow Agent.  |
| <i>interface-name</i>             | Interface of IPv4 address.                    |
| <b>ipv6</b> <i>interface-name</i> | Interface of IPv6 address.                    |

**Defaults** No sFlow Agent address is configured by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** This command is used to configure the Agent IP address field in the output sFlow datagram. The datagram not configured with this field cannot be output. The sFlow Agent address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Agent address, a message indicating configuration failure is displayed. It is recommended that the IP address of the sFlow Agent device be configured as the sFlow Agent address.

**Configuration Examples** The following example configures 192.168.2.1 as the sFlow Agent address.

```
Ruijie(config)# sflow agent address 192.168.2.1
```

**Verification** Use the show sflow command to display the sFlow configuration.

**Prompt** Prompt an error message when the address is invalid.

**Messages**      `invalid host address.`

**Common Errors**      N/A

**Platforms**      N/A

## 6.2 sflow collector *collector-id* destination

Use this command to configure the address of the sFlow Collector.

```
sflow collector collector-id destination { ip-address | ipv6 ipv6_address } udp-port [[vrf vrf-name] | [oob [via mgmt_mgmt-name]]]
```

Use this command to delete the address of the sFlow Collector.

```
no sflow collector collector-id destination { ip-address | ipv6 ipv6_address } udp-port [[vrf vrf-name] | [oob [via mgmt_mgmt-name]]]
```

Use this command to delete the address of the sFlow Collector.

```
default sflow collector collector-id destination { ip-address | ipv6 ipv6_address } udp-port [[vrf vrf-name] | [oob [via mgmt_mgmt-name]]]
```

### Parameter Description

| Parameter                        | Description                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <i>collector-id</i>              | sFlow Collector ID. The range is from 1 to 2.                                                                   |
| <i>ip-address</i>                | sFlow Collector IPv4 address                                                                                    |
| <b>ipv6</b> <i>ipv6-address</i>  | sFlow Collector IPv6 address                                                                                    |
| <i>udp-port</i>                  | sFlow Collector listening port number                                                                           |
| <b>vrf</b> <i>vrf-name</i>       | VRF instance name. It is not configured by default.                                                             |
| <b>oob</b>                       | The sampled traffics are output through the management interface. By default, this parameter is not configured. |
| <b>via</b> <i>mgmt_mgmt-name</i> | The name of management interface for sampled output.                                                            |

**Defaults**      No sFlow Collector address is configured by default.

**Command Mode**      Global configuration mode

**Default Level**      14

**Usage Guide**      This command is used to configure the sFlow Collector address. The sFlow Collector address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Collector address, a message indicating configuration failure is displayed. The sFlow Collector monitors the sFlow datagram on the specified port. When the vrf parameter is configured, the corresponding VRF instance must exist. When you remove the a VRF instance, the sFlow Collector

address will be removed if this VRF instance is also configured for an sFlow Collector address. When the oob parameter is configured, a datagram is sent to the sFlow Collector through the management interface.

**Configuration Examples** The following example configures 192.168.1.100 as the address of sFlow Collector 1, 6343 as the port number and vpn 1 as the VRF instance.

```
Ruijie(config)# sflow collector 1 destination 192.168.2.100 6343 vrf vpn1
```

**Verification** Use the **show sflow** command to display the sFlow Collector.

**Prompt Messages** Prompt an error message when the address is invalid.

```
invalid host address.
```

```
No VPN exists.
```

```
vpn is not exist
```

**Common Errors** N/A

**Platforms** N/A

### 6.3 sflow collector *collector-id* max-datagram-size

Use this command to configure the maximum length of the output sFlow datagram.

**sflow collector *collector-id* max-datagram-size *datagram-size***

Use this command to restore the default maximum length of the output sFlow datagram.

**no sflow collector *collector-id* max-datagram-size**

Use this command to restore the default maximum length of the output sFlow datagram.

**default sflow collector *collector-id* max-datagram-size**

| Parameter Description | Parameter                                        | Description                                                                      |
|-----------------------|--------------------------------------------------|----------------------------------------------------------------------------------|
|                       | <i>collector-id</i>                              | sFlow Collector ID. The range is from 1 to 2.                                    |
|                       | <b>max-datagram-size</b><br><i>datagram-size</i> | The maximum length of the output sFlow datagram. The range is from 200 to 9,000. |

**Defaults** The default maximum length of the output sFlow datagram is 1,400.

**Command Mode** Global configuration mode

**Default Level** 14

|                               |                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Usage Guide</b>            | N/A                                                                                                                                                                                   |
| <b>Configuration Examples</b> | The following example configures 1,000 as the maximum length of the output sFlow datagram for sFlow Collector.<br><pre>Ruijie(config)# sflow collector 1 max-datagram-size 1000</pre> |
| <b>Verification</b>           | Use the <b>show sflow</b> command to display the maximum length of the output sFlow datagram.                                                                                         |
| <b>Prompt Messages</b>        | N/A                                                                                                                                                                                   |
| <b>Common Errors</b>          | N/A                                                                                                                                                                                   |
| <b>Platforms</b>              | N/A                                                                                                                                                                                   |

## 6.4 sflow counter collector

Use this command to enable the sFlow Agent to send counter samples to the sFlow Collector.

**sflow counter collector** *collector-id*

Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector.

**no sflow counter collector**

Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector.

**default sflow counter collector**

| Parameter Description | Parameter           | Description                                   |
|-----------------------|---------------------|-----------------------------------------------|
|                       | <i>collector-id</i> | sFlow Collector ID. The range is from 1 to 2. |

**Defaults** Sending counter samples to the sFlow Collector is disabled by default.

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** This command can be used for physical ports, SVI ports and sub routed ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

**Configuration** The following example enables interface TenGigabitEthernet 0/5 to send counter samples to sFlow

|                        |                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------|
| <b>Examples</b>        | Collector 2.<br><pre>Ruijie(config-if-TenGigabitEthernet 0/5)# sflow counter collector 2</pre> |
| <b>Verification</b>    | Use the <b>show sflow</b> command to display the sFlow counter sampling configuration.         |
| <b>Prompt Messages</b> | N/A                                                                                            |
| <b>Common Errors</b>   | N/A                                                                                            |
| <b>Platforms</b>       | N/A                                                                                            |

## 6.5 sflow counter interval

Use this command to configure the sFlow counter sampling interval.

**sflow counter interval** *seconds*

Use this command to restore the default sFlow counter sampling interval.

**no sflow counter interval**

Use this command to restore the default sFlow counter sampling interval.

**default sflow counter interval**

| Parameter Description | Parameter      | Description                                                                                |
|-----------------------|----------------|--------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | sFlow counter sampling interval. The range is from 3 to 2,147,483,647. The unit is second. |

|                               |                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>               | The default sFlow counter sampling interval is 30 seconds.                                                                                              |
| <b>Command Mode</b>           | Global configuration mode                                                                                                                               |
| <b>Default Level</b>          | 14                                                                                                                                                      |
| <b>Usage Guide</b>            | This command is used to configure the global sFlow counter sampling interval, and sFlow Counter sampling of all interfaces uses this sampling interval. |
| <b>Configuration Examples</b> | The following example configures the sFlow counter sampling interval to 60 seconds.<br><pre>Ruijie(config)# sflow counter interval 60</pre>             |
| <b>Verification</b>           | Use the <b>show sflow</b> command to display the sFlow counter sampling interval.                                                                       |

**Prompt Messages** N/A

**Common Errors** N/A

**Platforms** N/A

## 6.6 sflow enable

Use this command to enable flow sampling and counter sampling on the interface.

**sflow enable [ ingress | egress ]**

Use this command to disable flow sampling and counter sampling on the interface.

**no sflow enable**

Use this command to disable flow sampling and counter sampling on the interface.

**default sflow enable**

| Parameter Description | Parameter      | Description                                  |
|-----------------------|----------------|----------------------------------------------|
|                       | <b>ingress</b> | Enables sFlow sampling in ingress direction. |
|                       | <b>egress</b>  | Enables sFlow sampling in egress direction.  |

**Defaults** The sFlow sampling function on an interface is disabled by default.

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** This command can be used to enable counter sampling and flow sampling for physical ports, SVI ports, sub routed ports and aggregate ports. sFlow datagram can be output only when an IP address is configured for the corresponding sFlow Collector.

If the direction parameter is not specified, sampling on both directions are enabled.

The SVI ports and sub routed ports support only the **ingress** parameter.

**Configuration Examples** The following example enables the sFlow sampling on interface TenGigabitEthernet 0/5.

```
Ruijie(config-if-TenGigabitEthernet 0/5)# sflow enable
```

**Verification** Use the **show sflow** command to display the status of the sFlow sampling function.

**Prompt Messages** N/A

**Common Errors** N/A

**Platforms** N/A

## 6.7 sflow flow collector

Use this command to enable the sFlow Agent to send flow samples to the sFlow Collector.

**sflow flow collector** *collector-id*

Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector.

**no sflow flow collector**

Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector.

**default sflow flow collector**

| <b>Parameter Description</b>  | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>collector-id</i></td> <td>sFlow Collector ID. The range is from 1 to 2.</td> </tr> </tbody> </table> | Parameter | Description | <i>collector-id</i> | sFlow Collector ID. The range is from 1 to 2. |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|---------------------|-----------------------------------------------|
| Parameter                     | Description                                                                                                                                                                                                     |           |             |                     |                                               |
| <i>collector-id</i>           | sFlow Collector ID. The range is from 1 to 2.                                                                                                                                                                   |           |             |                     |                                               |
| <b>Defaults</b>               | Sending the flow samples to the sFlow Collector is disabled by default.                                                                                                                                         |           |             |                     |                                               |
| <b>Command Mode</b>           | Interface configuration mode                                                                                                                                                                                    |           |             |                     |                                               |
| <b>Default Level</b>          | 14                                                                                                                                                                                                              |           |             |                     |                                               |
| <b>Usage Guide</b>            | This command can be used for physical ports, SVI ports, sub routed ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.        |           |             |                     |                                               |
| <b>Configuration Examples</b> | <p>The following example enables interface TenGigabitEthernet 0/5 to send flow samples to sFlow Collector 2.</p> <pre>Ruijie(config-if-TenGigabitEthernet 0/5)# sflow flow collector 2</pre>                    |           |             |                     |                                               |
| <b>Verification</b>           | Use the <b>show sflow</b> command to display the sFlow flow sampling configuration.                                                                                                                             |           |             |                     |                                               |
| <b>Prompt Messages</b>        | N/A                                                                                                                                                                                                             |           |             |                     |                                               |
| <b>Common Errors</b>          | N/A                                                                                                                                                                                                             |           |             |                     |                                               |
| <b>Platforms</b>              | N/A                                                                                                                                                                                                             |           |             |                     |                                               |

## 6.8 sflow flow max-header

Use this command to configure the maximum length of the packet header copied during flow sampling.

**sflow flow max-header** *length*

Use this command to restore the default maximum length of the packet header copied during flow

sampling.

**no sflow flow max-header**

Use this command to restore the default maximum length of the packet header copied during flow sampling.

**default sflow flow max-header**

**Parameter  
Description**

| Parameter     | Description                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------|
| <i>length</i> | Maximum length of the packet header to be copied. The range is from 18 to 256. The unit is byte. |

**Defaults** The default length is 64 bytes.

**Command  
Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Configure the maximum number of bytes of the packet content copied from the header of the original packet. The copied content is recorded in the generated sample.

**Configuration  
Examples** The following example sets the maximum length of the packet header copied during sFlow flow sampling to 128 bytes.

```
Ruijie(config)# sflow flow max-header 128
```

**Verification** Use the **show sflow** command to display the maximum length of the packet header copied during sFlow flow sampling.

**Prompt  
Messages** N/A

**Common  
Errors** N/A

**Platforms** N/A

## 6.9 sflow sampling-rate

Use this command to configure the sampling rate of sFlow flow sampling.

**sflow sampling-rate** *rate*

Use this command to restore the default the sampling rate of sFlow flow sampling.

**no sflow sampling-rate**



Use this command to restore the default sampling rate of sFlow flow sampling.

**default sflow sampling-rate**

| <b>Parameter Description</b>  | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>rate</i></td> <td>Sampling rate of sFlow sampling. One packet is sampled from every <i>n</i> packets (<i>n</i> equals the value of rate). The range is from 4,096 to 16,777,215.</td> </tr> </tbody> </table> | Parameter | Description | <i>rate</i> | Sampling rate of sFlow sampling. One packet is sampled from every <i>n</i> packets ( <i>n</i> equals the value of rate). The range is from 4,096 to 16,777,215. |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter                     | Description                                                                                                                                                                                                                                                                                                              |           |             |             |                                                                                                                                                                 |
| <i>rate</i>                   | Sampling rate of sFlow sampling. One packet is sampled from every <i>n</i> packets ( <i>n</i> equals the value of rate). The range is from 4,096 to 16,777,215.                                                                                                                                                          |           |             |             |                                                                                                                                                                 |
| <b>Defaults</b>               | The default sFlow flow sampling rate is 8,192.                                                                                                                                                                                                                                                                           |           |             |             |                                                                                                                                                                 |
| <b>Command Mode</b>           | Global configuration mode                                                                                                                                                                                                                                                                                                |           |             |             |                                                                                                                                                                 |
| <b>Default Level</b>          | 14                                                                                                                                                                                                                                                                                                                       |           |             |             |                                                                                                                                                                 |
| <b>Usage Guide</b>            | This command is used to configure the global sampling rate of sFlow flow sampling, and sFlow flow sampling of all interfaces uses this sampling rate.                                                                                                                                                                    |           |             |             |                                                                                                                                                                 |
| <b>Configuration Examples</b> | <p>The following example sets the sFlow flow sampling rate to 4,096.</p> <pre>Ruijie(config)# sflow sampling-rate 4096</pre>                                                                                                                                                                                             |           |             |             |                                                                                                                                                                 |
| <b>Verification</b>           | Use the <b>show sflow</b> command to display the sFlow flow sampling rate.                                                                                                                                                                                                                                               |           |             |             |                                                                                                                                                                 |
| <b>Prompt Messages</b>        | N/A                                                                                                                                                                                                                                                                                                                      |           |             |             |                                                                                                                                                                 |
| <b>Common Errors</b>          | N/A                                                                                                                                                                                                                                                                                                                      |           |             |             |                                                                                                                                                                 |
| <b>Platforms</b>              | N/A                                                                                                                                                                                                                                                                                                                      |           |             |             |                                                                                                                                                                 |

## 6.10 show sflow

Use this command to display the sFlow configuration.

**show sflow**

| <b>Parameter Description</b> | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table> | Parameter | Description | N/A | N/A |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|-----|-----|
| Parameter                    | Description                                                                                                                                           |           |             |     |     |
| N/A                          | N/A                                                                                                                                                   |           |             |     |     |
| <b>Command Mode</b>          | Privileged EXEC mode/global configuration mode/interface configuration mode                                                                           |           |             |     |     |
| <b>Default Level</b>         | 14                                                                                                                                                    |           |             |     |     |

**Usage Guide** N/A

**Configuration** The following example displays the sFlow configuration.

**Examples**

```
Ruijie(config)#show sflow
sFlow datagram version 5
Global information:
Agent IP: 10.10.10.10
sflow counter interval:30
sflow flow max-header:64
sflow sampling-rate:8192
Collector information:
ID IP Port Size VPN
1 192.168.2.100 6343 1400
2 NULL 0 1400
Port information
Interface CID FID Enable
TenGigabitEthernet 0/1 0 1 Y
TenGigabitEthernet 0/2 0 1 N
```

Field Description:

| Field                  | Description                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| sFlow datagram version | sFlow datagram version.<br>Currently, Ruijie supports V5 only.                                                                               |
| Agent IP               | IP address of the sFlow Agent. It can be configured by using the <code>sflow Agent address {ip-address   ipv6 ipv6-address }</code> command. |
| sflow counte interval  | Counter sampling interval                                                                                                                    |
| sflow flow max-header  | The maximum length of bytes of the packet header to be copied                                                                                |
| sflow sampling-rate    | Flow sampling rate                                                                                                                           |
| ID                     | sFlow Collector ID                                                                                                                           |
| IP                     | The IP address of the sFlow Collector to receive sFlow datagram                                                                              |
| Port                   | Port No. of the sFlow Collector to receive sFlow datagram                                                                                    |
| Size                   | The maximum length of the output sFlow datagram                                                                                              |
| VPN                    | VPN instance name of sFlow Collector                                                                                                         |
| Interface              | An interface configured with sFlow function                                                                                                  |
| CID                    | The destination sFlow Collector ID to which the sFlow Agent sends the counter samples.                                                       |
| FID                    | The destination sFlow Collector ID to which the sFlow Agent sends the flow samples.                                                          |
| Enable                 | The status of the sFlow sampling function                                                                                                    |

**Prompt Messages** N/A

**Platforms** N/A