Ruijie RG-S7808C Series Switches

RGOS Command Reference, Release 11.0(4)B2P2

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)B2P2

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

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related 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**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	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. CLI Authorization 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. CWMP Commands
9. Syslog Commands
10. CA-MONITOR Commands
11. Software Authorization Management Commands
12. Module Hot-plugging/unplugging Commands
13. Supervisor Module Redundancy Commands
14. USB/SD Commands
15. PoE Management Commands
16. UFT Commands
17. Package Management Commands

18. OpenFlow Commands

1 CLI Authorization Commands

1.1 alias

	Use this command to configure a command alias in global configuration mode. Use the **no** form of this command to remove the alias of a specified command or all the aliases in a specified mode.
	alias *mode command-alias original-command*
	no alias *mode command-alias*

Parameter Description	**Parameter**	**Description**
	mode	Mode of the command represented by the alias
	command-alias	Command alias
	original-command	Syntax of the command represented by the alias

Defaults	Some commands in 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	#In global configuration mode, use def-route to represent the default route setting of ip route 0.0.0.0 0.0.0.0 192.168.1.1: `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` `globle 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	Shows 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 execution rights of a command to the default setting.
	privilege *mode* [**all**] [**level** *level* **| reset**] *command-string*
	no privilege *mode* [**all**] [**level** *level*] *command-string*

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

#Set the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

```
Ruijie(config)#enable secret level 1 0 test
Ruijie(config)#privilege exec level 1 reload
After the above setting, 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 Description	N/A.	

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**
	mode	Mode of the command represented by the alias.
Defaults	N/A.	
Command Mode	EXEC mode.	
Usage Guide	Show the configuration of all aliases if no command mode is input.	
Configuration Examples	#Show the command alias in EXEC mode: 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 Description	N/A.	

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 the EXEC 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.

	message	Contents of the message.
Defaults	N/A	
Command Mode	Global configuration 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 Examples	The following example configures the EXEC message. `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 the incoming message for reverse Telnet session. Use the **no** form of this command to restore the default setting.	
	banner incoming *c message c*	
	no banner incoming	
Parameter Description	**Parameter**	**Description**
	c	Separator of the message. Delimiters are not allowed in the message.
	message	Contents of the message.
Defaults	N/A	
Command Mode	Global configuration mode	

Usage Guide	This command is used to configure the coming 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.
Configuration Examples	The following example configures the banner incoming message for reverse Telnet session. `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 the login banner. Use **no** form of this command to r restore the default setting.
	banner login *c message c*
	no banner login

Parameter Description	**Parameter**	**Description**
	c	Separator of the message contained in the login banner. Delimiters are not allowed in the MOTD.
	message	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 Examples	The following example configures the login banner. `Ruijie(config)# banner login $ enter your password $`	

Related	**Command**	**Description**

Commands		
	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 restore the default setting.	
	banner [**motd**] *c message c*	
	no banner [**motd**]	
Parameter Description	**Parameter**	**Description**
	c	Separator of the MOTD. Delimiters are not allowed in the MOTD.
	message	Contents of an MOTD
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command sets the MOTD, which is displayed at login. The letters that follow the separator will be discarded.	
Configuration Examples	The following example configures the MOTD. `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 prompt authentication timeout. Use the **no** form of this command to restore the default setting.
	banner prompt-timeout *c message c*
	no banner prompt-timeout

Parameter Description	**Parameter**	**Description**
	c	Separator of the message. Delimiters are not allowed in the message.
	message	Contents of the message.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure the prompt-timeout message. The system discards all the characters next to the terminating symbol. When authentication times out, the banner prompt-timeout message is displayed.	
Configuration Examples	The following example configures the prompt-timeout message to prompt authentication timeout. `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 restore the default setting.	
	banner slip-ppp *c message c*	
	no banner slip-pp	
Parameter Description	**Parameter**	**Description**
	c	Separator of the message. Delimiters are not allowed in the message.
	message	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 Examples	The following example configures the banner slip-ppp message for the SLIP/PPP session. `Ruijie(config)# banner slip-ppp $ Welcome $`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

2.8 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**
	cp-name	(Optional) Specifies the checkpint name. in the range from 1 to 80 characters.
	description *description*	(Optional) specifies the checkpoint description, in the range from 1 to 80 characters.

Defaults	N/A
Command Mode	Privileged EXEC 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 Examples	The following example creates a checkpoint with a default name. `Ruijie# checkpoint` `...` `user-checkpoint-1 created Successfully`

Related	**Command**	**Description**

Commands		
	N/A	N/A
Platform Description	N/A	

2.9 clear checkpoint database

	Use this command to clear the checkpoint statistics.	
	clear checkpoint database	
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 the checkpoint statistics. `Ruijie# clear checkpoint database`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.10 clock set

	Use this command to set the system clock manually.	
	clock set *hh*:*mm*:*ss* **month day year**	
Parameter Description	**Parameter**	**Description**
	hh:*mm*:*ss*	Current time: Hour (24-hour): Minute: Second
	day	Date (1-31) of month
	month	Month (1-12) of year

	year	Year (1993-2035): No abbreviation is allowed.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to set the system time to facilitate management. For devices without hardware clock, the time set by the clock set command applies only for the current setting. Once the device is powered off, the set time becomes invalid.	
Configuration Examples	The following example configures the current time as 10:20:30AM March 17th 2003. `Ruijie# clock set 10:20:30 Mar 17 2003` `Ruijie# show clock` `clock: 2003-3-17 10:20:32`	
Related Commands	**Command**	**Description**
	show clock	Displays current clock.
Platform Description	N/A	

2.11 clock update-calendar

	Use this command to overwrite the value of hardware clock by software clock.	
	clock update-calendar	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Some platforms use hardware clock as a complement. As the battery enables hardware clock to run continuously hardware clock still runs, whether the device is turned off or restarted. If hardware clock and software clock are out of sync, the software clock is more reliable. Execute the **clock update-calendar** command to copy the date and time indicated by the software clock to the hardware clock.	

Configuration Examples	The following example copies the current time and date indicated by the software clock to the hardware clock. `Ruijie# clock update-calendar`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

2.12 configure

	Use this command to enter global configuration mode.
	configure [**terminal**]
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 enters global configuration mode. `Ruijie# configure` `Ruijie(config)#`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

2.13 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

2.14 disconnect

	Use this command to disconnect the Telnet Client session.
	disconnect *session-id*

Parameter Description	**Parameter**	**Description**
	session-id	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. `Ruijie# disconnect 1`

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** *leve l*]	
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 Examples	The following example configures the password as **pw10**. `Ruijie(config)# enable password pw10`	
Related Commands	**Command**	**Description**
	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 Mode	Global configuration 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 Examples	The following example configures the security password as **pw10**. `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 Examples	The following example enables the SSH Server. `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 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 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. 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 Examples	The following example disables display of the EXEC message on line VTY 1. `Ruijie(config)# line vty 1` `Ruijie(config-line)no exec-banner`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.20 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	**Parameter**	**Description**

Description		
	minutes	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 Examples	The following example sets the connection timeout to 5'30". `Ruijie(config-line)#exec-timeout 5 30`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.21 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 Examples	The following example displays brief information about the help system. `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
  dldp            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 Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.22 hostname

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

Parameter Description	Parameter	Description
	name	Device hostname, string, number or hyphen, up to 63 characters.
Defaults	The default is Ruijie.	
Command Mode	Global configuration 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

2.23 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**
	interface-name / 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 connetction. 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

2.24 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 Examples	The following example locks a terminal interface. `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

2.25 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 Mode	This function is disabled by default.
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 Examples	The following example enables terminal locking at the console port and locks the console. `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	

2.26 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 Examples	The following example sets a login password authentication on VTY.. `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	

2.27 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
	list-name	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

2.28 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 Examples	The following example sets local user authentication on VTY. `Ruijie(config)# no aaa new-model` `Ruijie(config)# username test password 0 test` `Ruijie(config)# line vty 0` `Ruijie(config-line)# login local`

Related Commands	Command	Description
	username	Configures local user information.
Platform Description	N/A	

2.29 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. 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 Examples	The following example disables display of the MOTD message on VTY 1. `Ruijie(config)# line vty 1` `Ruijie(config-line)no motd-banner`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.30 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**
	password	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.
	encrypted-password	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 Examples	The following example configures the line login password as "red". `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	

2.31 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 Examples	The following example sets the prompt string to rgnos. `Ruijie(config)# prompt rgnos` `Ruijie(config)# end` `RGOS`	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.32 reload

	Use this command to restart the device system.
	reload [*text* | **in** [*hh:*] *mm* [*text*] | **at** *hh:mm* [*month day year*] [*text*] | **cancel**]

Parameter Description	Parameter	Description
	text	Causes the system to restart, 1-255 bytes
	in [*hh:*] *mm*	The system is restarted after a specified time interval of up to 24 days.
	at *hh:mm*	The system is restarted at the specified time.
	month	Indicates a month using characters, such as Mar for March.
	day	Date in the range from 1 to 31
	year	Year in the range from 1993 to 2035. No abbreviation is allowed.
	cancel	Cancels the scheduled restart.
Defaults	N/A	
Command	Privileged EXEC mode	

Mode	
Usage Guide	This command is used to restart the device at a specified time to facilitate management.
Configuration Examples	The following example restarts the system in 10 minutes. `Ruijie# reload in 10` `Router will reload in 600 seconds.`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.33 rollback

	Use this command to roll back the checkpoint configuration.
	rollback running-config checkpoint *cp-name* [**display-differences** | **ignore-results**]

Parameter Description	**Parameter**	**Description**
	cp-name	Specifies the checkpoint name, in the range from 1 to 80 characters.
	display-differences	Displays configuration difference after the rollback is comple. 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.
Configuration Examples	The following example rolls back the configuration of checkpoint user-1. `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	

2.34 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.
	password	Sets the password plaintext, a string ranging from 1 to 25 characters.
	5 *encrypted-secret*	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 Examples	The following example sets the password encrypted by irreversible MD5 for line login to vty0. `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 Description	N/A

2.35 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 *device-number*	Sets the device number.
	slot { **m1 | m2** }	Sets the management module to either m1 or m2.
	slot *slot-number*	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	

2.36 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**
	minutes	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	

2.37 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**
	cp-name	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 Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration 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	

2.38 show clock

	Use this command to display the system time.
	show clock

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 current system clock.	
Configuration Examples	The following example displays a result of the **show clock** command. `Ruijie# show clock` `clock: 2003-3-17 10:27:21`	
Related Commands	**Command**	**Description**
	clock set	Sets the system clock.
Platform Description	N/A	

2.39 show line

	Use this command to display the configuration of a line.	
	show line { **console** *line-num* | **vty** *line-num* | *line-num* }	
Parameter Description	**Parameter**	**Description**
	console	Display s the configuration of a console line.
	vty	Display s the configuration of a vty line.
	line-num	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

2.40 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 Examples	The following example displays the restart settings of the system. Ruijie# **show reload** Reload scheduled in 595 seconds. At 2003-12-29 11:37:42 Reload reason: test.
Related	**Command** / **Description**

Commands		
	N/A	N/A
Platform Description	N/A	

2.41 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 Examples	N/A	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.42 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 Examples	The following example displays whether the service is enabled or disabled. `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	

2.43 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 Examples	The following example displays the Telnet Client session information. `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	

2.44 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 Examples	N/A	
Related Commands	Command	Description
	boot config	Sets the name of the boot configuration file.
Platform Description	N/A	

2.45 show this

	Use this command to display effective configuration in the current mode.	
	show this	
Parameter Description	**Parameter**	**Description**
	N/A	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. Use the **line** *first-line last-line* command to configure lines in a continuous group and enter LINE configuration mode. Use the **vlan range** command to configure VLANs and enter vlan range configuration mode. Use the **interface range** command to configure interfaces and enter interface range configuration mode.	
Configuration Examples	`Use this command to display effective configuration on interface fastEthernet 0/1.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	

2.46 show version

	Use this command to display information about the system.	
	show version [**devices** | **module** | **slots**]	
Parameter Description	**Parameter**	**Description**
	devices	Current information about the device.
	module	Current information about the module.
	slots	Current information about the slot.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to view current system information, including the system start time, version, device information, and serial number.	
Configuration Examples	The following example displays system information. `Ruijie# show version` `System description : Ruijie Dual Stack Multi-Layer Switch(S3760-24) By Ruijie Network` `System start time: 1970-6-14 11:49:53` `System uptime: 3:17:1:17` `System hardware version: 2.0` `System software version: RGOS 10.3.00(4), Release(34679)` `System boot version: 10.2.34077` `System CTRL version: 10.2.24136` `System serial number: 1234942570001`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.47 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**
	speed	Transmission rate (bps) on the terminal. For serial ports, optional rates include 9600, 19200, 38400, 57600, and 115200 bps. The default rate is 9600 bps.
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	

2.48 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::X* | **interface** *interface-name* }] [**/vrf** *vrf-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 A.B.C.D	Specifies the source IPv4 address used by the Telnet client.
	ipv6 X:X:X:X::X	Specifies the source IPv6 address used by the Telnet client.
	interface *interface-name*	Specifies the source interface used by the Telnet client.
	/vrf *vrf-name*	Specifies the VRF routing table you want to query.

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to log in a telnet server.
Configuration Examples	The following example sets telnet to 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 2AAA:BBBB::CCCC. `Ruijie# telnet 2AAA:BBBB::CCCC`

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	

2.49 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** { **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**
	name	Username
	login mode	Sets the login mode.
	console	Sets the login mode to console.
	ssh	Sets the login mode to ssh.
	telnet	Sets the login mode to telnet.
	online amount *number*	Sets the amount of users online simultaneously.

	permission *oper-mode path*	Sets the permission on the specified file. *op-mode* refers to the operation mode and *path* to the file or the directory path.
	privilege *privilege-level*	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**] *text-string*	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. If encryption type is 7, the cipher text you enter should contain seven characters to be valid. In general, do not set the entryption type 7. Instead, specify the type of encryption as 7 only when the encrypted password is copied and pasted.	
Configuration Examples	The following example configures a username and password and binds the user to level 15. `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 confix.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 Description	N/A	

2.50 username import

	Use this command to import user information from the file.	
	username import *filename*	
Parameter Description	**Parameter**	**Description**
	filename	The file name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to import user information from the file.	
Configuration Examples	The following example imports user information from the file. `Ruijie# username import user.csv`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.51 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 Examples	The following example exports user information to the file. `Ruijie# username export user.csv`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

2.52 write

	Use this command to save **running-config** at a specified location.
	write [**memory | terminal**]
Parameter Description	**Parameter** / **Description** **memory** / Writes the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**. **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 Examples	The following example saves **running-config** at a specified location. `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**
	access-list-number	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.
	access-list-name	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**
	level	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
	default	Default authorization list name.
	list-name	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 commands *level* { **default** | *list-name* }
	no accounting commands *level*

Parameter Description	Parameter	Description
	level	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
	default	Default authorization list name.
	list-name	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 Examples	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 perform authorization on commands, Use the **no** form of this command to restore the default setting.
	c *level* { **default** | *list-name* }
	no authorization commands *level*

Parameter Description	Parameter	Description
	level	Command level ranging from 0 to 15. The command of this level is executed after authorization is performed.
	default	Default authorization list name,
	list-name	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 Examples	The following example performs authorization on commands of level 15 in line VTY 1. `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 Description	N/A	

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,
	list-name	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 authorization first, and then apply it on the line.
Configuration Examples	The following example performs EXEC authorization to line VTY 1. `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 Commands	**Command** / **Description**
	N/A / N/A
Platform Description	N/A

3.6 clear line

	Use this command to clear connection status of the line.
	clear line { **console** *line-num* | **vty** *line-num* **|** *line-num* }
Parameter Description	**Parameter** / **Description**
	console / Clears connection status of the console line.
	vty / Clears connection status of the virtual terminal line.
	line-num / 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 Description	N/A

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**
	ascii-value	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. Use the **no** form of this command to restore the default setting.	
	escape-character *escape-value*	
	no escape-character	
Parameter Description	**Parameter**	**Description**
	escape-value	ASCII decimal value of the escape character, 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 Examples	The following example sets the escape character to 23 (**Ctrl+w**). `Ruijie(config)# line vty 0` `Ruijie(config-line)# escape-character 23`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

3.9 exec

	Use this command to allow 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 Examples	The following example bans line VTY 1 from entering the command line interface. `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 Commands	**Command** / **Description**
	N/A / N/A
Platform Description	N/A

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	**Command** / **Description**

Commands		
	N/A	N/A
Platform Description	N/A	

3.11 ipv6 access-class

	Use this command to control login into 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**
	access-list-name	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**
	screen-length	Screen length, in the range from 0 to 512.

Defaults	The default is 24.
Command Mode	Line configuration mode
Usage Guide	N/A
Configuration Examples	The following example sets the screen length to 10. `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.
	first-line	Number of first-line to enter
	last-line	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 Examples	The following example enters the LINE mode from LINE VTY 1 to 3: `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** N/A / N/A
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**
	location	Line location description
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example describes the line location as Swtich's Line Vty 0. `Ruijie(config)# line vty 0` `Ruijie(config-line)# location Swtich's Line Vty 0`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

3.16 monitor

	Use this command to support log print 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 Examples	The following example supports log print on the terminal in VTY line 0 5. `Ruijie(config)# line vty 0 5` `Ruijie(config-line)# monitor`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

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**
	level	Privilege level, in the range from 0 to 15.
Defaults	The default is 1.	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the privilege level for the line VTY 0 4 to 14. `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**
	c	Delimiter of the login refusal message, which is not allowed within the message.
	message	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	**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 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 Description	N/A	

3.20 show line

	Use this command to display line configuration.	
	show line { **console** *line-num* | **vty** *line-num* **|** *line-num* }	
Parameter Description	**Parameter**	**Description**
	console	Displays configuration for the console line.
	vty	Displays configuration for the virtual terminal line.
	line-num	Displays the line.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration Examples

The following example displays configuration for the 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
```

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 Description	N/A

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 Examples	The following example displays the privilege level of the line. `Ruijie# show privilege` `Current privilege level is 10`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

3.22 show user

	Use this command to display the login user information.	
	show user [**all**]	
Parameter Description	**Parameter**	**Description**
	all	Displays line user information, including users logging into the line and users not logging into the line.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A
Configuration Examples	The following example displays the information about users logging into the line, `Ruijie# show user` `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 user 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 Description	N/A	

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**
	baudrate	Sets the baud rate, in the range from 9600 to 115200.
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 Description	N/A

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**
	escape-value	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	N/A

Description	

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**
	size *size*	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 Mode	Privileged EXEC 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 Description	N/A	

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**
	screen-length	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 Description	N/A	

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**
	location	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 “Swtich’s Line Vty 0”. `Ruijie# terminal location Swtich’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
	baudrate	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 Examples	The following example sets the baud rate for the current terminal to 115200, `Ruijie# terminal speed 115200`	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.29 terminal width

	Use this command to set the screen width for the terminal.	
	terminal width *screen-width*	
	terminal no width	
Parameter	Parameter	Description

Description		
	screen-width	Sets the screen width for the terminal, in the range from 0 to 256.
Defaults	The default is 79.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the screen width for the terminal to 10. `Ruijie# terminal width 10`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

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.
	seconds	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 Examples	The following example sets the login authentication timeout to 300 seconds for line VTY 0 5. `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 5` `Ruijie(config-line)transport input ssh`
Related Commands	**Command** / **Description**
	show running / Displays status information
Platform Description	N/A

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**
	c	Delimiter of the logout message, which is not allowed within the message.
	message	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	This command is used to set the logout message to “Logout from the ruijie device”. `Ruijie(config-line)#vacant-message @ Logout from the ruijie device @`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

3.33 width

	Use this command to set the screen width. Use the **no** form of this command to restore the default setting,	
	width *screen-width*	
	no width	
Parameter Description	**Parameter**	**Description**
	screen-width	Screen width, in the range from 0 to 256,

Defaults	The default is 79.	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the screen width to 10. `Ruijie(config-line)# width 10`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4 File System Commands

4.1 cd

	Use this command to set the present directory for the file system.	
	cd *[filesystem:] [directory]*	
Parameter Description	**Parameter**	**Description**
	filesystem:	The URL of filesystem, followed by a colon (:). The filesystem includes **flash:**, **sata:**, **usb:**, **sd:** and **tmp:**.
	directory	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 Mode	Privileged EXEC 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	The following example enters the sata hardware. `Ruijie#pwd` `flash:/` `Ruijie#cd sata:` `Ruijie#pwd` sata:/	
Related Commands	**Command**	**Description**
	pwd	Displays the present word directory.
Platform Description	N/A.	

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*

<table>
<tr><td>Parameter Description</td><td>Parameter</td><td>Description</td></tr>
<tr><td></td><td>source-url</td><td>Source file URL, which can be local or remote.</td></tr>
<tr><td></td><td>destination-url</td><td>Destination file URL, which can be local or remote.</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Defaults</td><td colspan="2">N/A.</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Command Mode</td><td colspan="2">Privileged EXEC mode.</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Usage Guide</td><td colspan="2">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:
<table>
<tr><th>Prefix</th><th>Description</th></tr>
<tr><td>running-config</td><td>Running configuration file.</td></tr>
<tr><td>startup-config</td><td>startup configuration file.</td></tr>
<tr><td>flash:</td><td>local FLASH file system.</td></tr>
<tr><td>tftp:</td><td>The URL of TFTP network server, in the format as follows:
tftp:[[//location]/directory]/filename</td></tr>
<tr><td>oob_tftp:</td><td>The URL of TFTP network server connected with the Out-of-Band port,</td></tr>
<tr><td>xmodem:</td><td>Files on the network device using the xmodem protocol.</td></tr>
</table></td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Configuration Examples</td><td colspan="2">The following example copies the netconfig file from device 192.168.64.2 to the FLASH disk and the netconfile file exists locally.
<pre>
Ruijie#copy tftp://192.168.64.2/netconfig flash:/netconfig
The file [flash:/netconfig] exits,override it? [Y/N]: y
Copying: !!!!!!!!

Accessing tftp://192.168.64.2/netconfig finished, 2399bytes prepared
Flushing data to flash:/netconfig…
Flush data done
</pre></td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Related Commands</td><td>Command</td><td>Description</td></tr>
<tr><td></td><td>delete</td><td>Deletes the file.</td></tr>
<tr><td></td><td>rename</td><td>Renames the file.</td></tr>
<tr><td></td><td>dir</td><td>Displays the file list of the specified directory.</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Platform Description</td><td colspan="2">N/A</td></tr>
</table>

4.3 delete

	Use this command to delete the files in the present directory.	
	delete [*filesystem*:] *file-url* [/**force** | /**recursive**]	
Parameter Description	**Parameter**	**Description**
	filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **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.
	/**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 Mode	Privileged EXEC 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 Examples	The following example deletes the fstab file on the FLASH disk.	

```
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 Description	N/A	

4.4 dir

	Use this command to display the files in the present directory.	
	dir [*filesystem*:] [*directory*]	
Parameter Description	**Parameter**	**Description**
	filesystem	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, **sd:** and **tmp:**.
	directory	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: ● 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 Description

N/A.

4.5 erase

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

erase *filesystem*

Parameter Description

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

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples	The following example erases the USB filesystem. `Ruijie#erase usb0:` `Sure to erase usb0:? [Y/N] y` `Erasing disk usb0 …` `Erase disk usb0 done!`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.6 file

	Use this command to display the information about a file.
	file [*filesystem*:] *file-url*

Parameter Description	**Parameter**	**Description**
	filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **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 Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	The following example displays the information about gcc executable file. `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

4.7 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 Examples	The following example sets the prompt mode to noisy. `Ruijie#file prompt noisy`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.8 mkdir

	Use this command to create a directory.	
	mkdir [*filesystem*:] *directory*	
Parameter Description	**Parameter**	**Description**
	filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, **sd:** and **tmp:**.
	directory	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 Mode	Privileged EXEC 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 Examples	The following example creates a directory named 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)` `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 Description	N/A	

4.9 more

	Use this command to display the content of a file.	
	more [/**ascii** | /**binary**] [*filesystem*:] *file-url*	
Parameter Description	**Parameter**	**Description**
	/**ascii**	Displays the file content in the ASCII format.
	/**binary**	Displays the file content in the
	filesystem:	The URL of file system, followed by a colon (:). The file system

		includes **flash:**, **sata:**, **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 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> <protofamily> <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 Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.10 rename

	Use this command to move or rename the specified file.
	rename src-url dst-url

Parameter Description	Parameter	Description
	src-url	The source file URL to move.
	dst-url	The URL of the destination file or directory.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example renames the fstab file in the root directory on the FLASH disk as new-fstab. `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 Description	N/A	

4.11 rmdir

	Use this command to delete an empty directory.	
	rmdir [*filesystem*:] *directory*	
Parameter Description	**Parameter**	**Description**
	filesystem:	The URL of file system, followed by a colon (:). The file system

		includes **flash:**, **sata:**, **usb:**, **sd:** and **tmp:**.
	directory	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 Examples	The following example deletes the null test directories. `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 Commands	**Command**	**Description**
	N/A.	N/A.
Platform Description	N/A.	

4.12 pwd

	Use this command to display the working path.
	pwd

Parameter Description	Parameter	Description
	N/A.	N/A.
Defaults	N/A.	
Usage Guide	This command displays the present working path	
Configuration Examples	The following example displays the process of switching the working directory from flash: to sata:. `Ruijie#pwd` `flash:/` `Ruijie#cd sata:/` `Ruijie#pwd` sata:/	
Related Commands	**Command**	**Description**
	cd	Changes the file system in the present directory.
Platform Description	N/A.	

4.13 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 Examples	The following example displays the file system information: `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: ● ro: read-only ● wo: write-only ● rw: read and write
Prefixes	File system prefix

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

4.14 show mount

	Use this command to display the mounted information.
	show mount

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults	N/A
Command Mode	N/A
Usage Guide	N/A
Configuration Examples	The following example displays the mounted information.

```
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 Description	N/A

4.15 tree

	Use this command to display the file tree of the current directory.
	tree [*filesystem*:] [*directory*]

Parameter Description	Parameter	Description
	filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, **sd:** and **tmp:**.
	directory	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	N/A
Configuration Examples	The following example displays the file tree of flash:/echo `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 Commands	Command	Description
	N/A	N/A

Platform Description	N/A

4.16 verify

	Use this command to compute, display and verify Message Digest 5 (MD5).	
	verify [**/md5** *md5-value*] *filesystem***:** [*file-url*]	
Parameter Description	**Parameter**	**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:**, **sata:**, **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 Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example computes MD5 of flash:/gcc. `Ruijie#verify flash:/gcc` `8b072de7db7affd8b2ef824e7e4d716c` The following example	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.17 show disk

	Use this command to display sata/USB/Flash information.	
	show disk *sata*/*usb*/*flash*	
Parameter Description	**Parameter**	**Description**
	sata	Displays hardware information.

	usb	Displays USB information.
	flash	Displays FLASH information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays sata information. `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 Description	N/A	

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**
	hour [:minute [:second]]	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.
	month	Sets month. The range is from 1 to 12.
	day	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
	year	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 **calendar 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 **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	1: 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` 2: 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` 3: 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	1: 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**
	hour [:minute [:second]]	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.
	month	Sets month. The range is from 1 to 12.
	day	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
	year	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. 19. 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	1: The following example changes the current software time of the system (for example, 2012-02-01	

Examples	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` 2: 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` 3: 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.
	start-month	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.
	week	Start week in the start month. The range is from 1 to 5.
	last	The last week of the specified month.
	start-date	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.
	end-month	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.
	hours-offset	Hours ahead of the standard time. The range is from 0 to 12. You are not allowed to set it to 00:00.
	minutes-offset	Minutes ahead of the standard time. The range is from 0 to 59. If *hours-offset* has been set to 0, you are not allowed to set *minutes-offset* 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	1: 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` 2: 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` 3: Disable 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**
	name	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.
	hours-offset	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 *hours-offset*.
	minutes-offset	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	1: 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` 2: 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)` 3. 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	1: 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.` 2: 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` 3: 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 *high-value*	Sets the high watermark of the CPU usage. The range is from 2 to 99.
	range *range-value*	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	This command is supported only in VSD0 mode. Multiple VSDs are not supported. 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.	
Configuration Examples	1: The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled). `Ruijie(config)# default cpu high-watermark set` `Reset default cpu watermark monitor` `set system cpu watermark high 80%(75%~85%)` 2: The following example disables CPU usage monitoring. `Ruijie(config)# no cpu high-watermark set` `Close cpu watermark monitor` 3: The following example enables CPU usage monitoring. Keep the defined watermark value. `Ruijie(config)# cpu high-watermark set` `Open cpu watermark monitor` `set system cpu watermark high 80%(75%~85%)` 4: The following example enables CPU usage monitoring and sets the high watermark to 88% and fluctuation range to 3%. `Ruijie(config)# cpu high-watermark set high 88 range 3` `Open cpu watermark monitor` `set system cpu watermark high 88%(85%~91%)` 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%).	
Check Method	-	
Prompt	If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the	

Message	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 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-value*	
	Use this command to disable the detection of memory low watermark. **no memory low-watermark set**	
Parameter Description	**Parameter**	**Description**
	mem-value	Memory watermark threshold. The range is from 1 KB to 4,294,967,295 KB.
Defaults	By default, the detection of memory low watermark is disabled.	
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 Examples	1: The following example sets the low watermark threshold of the memory to 500,000 KB and enables detection. Ruijie(config)#memory low-watermark 500000	
Check Method	-	
Prompt Message	When the system memory is less than the defined watermark value (such as 500000 KB), the system prints the following message: Ruijie(config)#<187> Jan 1 00:18:59 syslog: Free Memory has dropped below 500000k	

Platform Description	-

5.9 memory history clear

	Use this command to clear the history of the memory usage. **memory history clear** [**one-forth | half | all**]	
Parameter Description	**Parameter**	**Description**
	one-forth	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	1: 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	-

5.10 reload

	Use this command to reload the device. **reload** [**at** { *hour* [:*minute* [:*second*]] }	
Parameter Description	**Parameter**	**Description**
	hour [:*minute* [:*second*]]	Sets the restart time in the format of hour : minute : second. Other neglected parameters keep the current system values.
Defaults	-	
Command Mode	Privileged EXEC mode	
Default Level	-	
Usage Guide	-	
Configuration Examples	The following example reloads the device. 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 Description	**Parameter**	**Description**
	-	-
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	-	
Configuration Examples	The following example displays the hardware calendar. `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 Description	**Parameter**	**Description**
	-	-
Command Mode	Privileged EXEC mode / global configuration mode	
Default Level	-	

Usage Guide	-
Configuration Examples	1. The following example displays the software clock when the time zone is disabled. `Ruijie# show clock` `18:22:20 UTC Tue, Dec 11, 2012` 2. 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 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.
	process-id	Displays the memory usage of the task specified by *process-id*.
	process-name	Displays the memory usage of the task specified by *process-name*.

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	1: 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	-

5.14 show memory vsd

	Use this command to display memory information. **show memory vsd** *vsd_id*	
Parameter Description	**Parameter**	**Description**
	vsd_id	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 Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	This command is supported only in VSD0 mode.	
Configuration	1: 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	-

5.15 show pci-bus

	Use this command to display the information on the device mounted to the PCI bus. **show pci-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 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	-

5.16 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	1: 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--
```

2: 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.

3: The following example displays the CPU usage in ascending order of task IDs and only the processes with non-zero CPU usage within 15 minutes are displayed.

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

4: The following example displays the CPU usage in descending order within five seconds and the tasks with zero CPU usage within one second are not displayed.

```
Ruijie #show processes cpu 5sec nonzero
```

5: The following example displays the CPU usage of the control core in histograms within the last 60 seconds, 60 minutes, and 72 hours.

The first histogram displays the CPU usage of the control core within 300 seconds. Every segment in the x-coordinate is five seconds, and every segment in the y-coordinate is 5%. The symbol "*" indicates the CPU usage at the last specified second. In other words, the first segment on the x-coordinate nearest to 0 is the CPU usage in the last five seconds, measured in %.

The second histogram displays the CPU usage of the control core within the last 60 minutes, measured in %. Every segment on the x-coordinate is 1 minute.

The third histogram displays the CPU usage of the control core within the last 72 hours, measured in %. Every segment on the x-coordinate is 1 hour.

Example:

```
Ruijie#show processes cpu history


            system cpu percent usage(%) [last 300 second]

    -
  100|
   95|
   90|
   85|
   80|
   75|
   70|
   65|
   60|
   55|
   50|
   45|
   40|*********
   35|||||||||
   30|||||||||*
   25||||||||||
   20||||||||||
   15||||||||||
   10||||||||||
    5||||||||||***************
    0|||||||||||||||||||||||||
     #========#========#=====*==>
```

```
    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)
------------------------------------------------------------------------------
```

6: 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	-

5.17 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**
	process-id	Displays the information on the task of the specified task ID.
	process-name	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 Examples	1: The following example displays the information on the task of the specified task name. `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

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

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

Prompt Message	-
Platform Description	-

5.18 show processes vsd

	Use this command to display system task of the specified VSD. **show process vsd** *vsd_id* **cpu**

Parameter Description	**Parameter**	**Description**

	vsd_id	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	1: The following example displays the system task information in VSD1 mode. `Ruijie#show processes vsd 1 cpu`	
Prompt Message	-	
Platform Description	-	

5.19 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	-	

5.20 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	-

5.21 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	1: 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	-

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 *time date*	Indicates the start time of the range.
	end *time date*	Indicates the end time of the range.

Defaults	The default absolute time range is the maximum range, which is from 00:00 January 1, 0 to 23:59 December 31, 9999.
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. The maximum absolute time range is from 00:00 January 1, 0 to 23:59 December 31, 9999.
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**
	day-of-the-week	Indicates the week day when the periodic time starts or ends.
	time	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 Description	**Parameter** / **Description**
	time-range-name / 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. `Ruijie# show time-range` `time-range entry: test (inactive)` `absolute end 01:02 02 February 2012`
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 Description	**Parameter** / **Description**
	time-range-name / 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 Examples	The following example creates a time range. `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 upgrade web

	Use this command to upgrade the Web package in local file system.	
	upgrade web *uri*	
Parameter Description	**Parameter**	**Description**
	uri	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 Examples	The following example copies a Web package into the file system and upgrades the package. `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 Description	N/A	

7.2 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**
	oob_tftp: *path*	*path* indicates the storage path of the Web package on the TFTP server. **oob_tftp** indicates the system downloads the Web package from the

		TFTP server through the MGMT port and upgrades the Web package automatically. This parameter is supported only on the the device supporting the MGMT port.
	tftp: *path*	*path* indicates the storage path of the Web package on the TFTP server. **tftp** indicates the system downloads the Web package from the TFTP server through the physical port and upgrades the Web package automatically.
Defaults	N/A	
Command mode	Global configurationPrivileged 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 Description	N/A	

8 CWMP Commands

8.1 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**
	password	Configures the ACS user password to be authenticated for the CPE to connect to the ACS.
	encryption-type	Specifies the encryption type, which can be set to **0** (indicating that no encryption is used) or **7** (indicating that simple encryption is used).
	encrypted-password	Specifies the password in encrypted form.
Defaults	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` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
	acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.
Platform Description	N/A	

8.2 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 device to the default factory setting.	
	acs url *url*	
	no acs url	
Parameter Description	**Parameter**	**Description**
	url	Specifies the URL of the ACS.
Defaults	N/A	
Command mode	CWMP configuration 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 in http://ip [: port]/ path" format. ● The URL of the ACS consists of at most 256 characters	
Configuration Examples	The following example specifies the URL of the ACS 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)#acs url http://10.10.10.1:7547/acs` `Ruijie(config-cwmp)#`	
Related Commands	**Command**	**Description**
	show cwmp configuration	Shows the current configuration of CWMP.

	show cwmp status	Shows the running status of CWMP.
Platform Description	N/A	

8.3 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 device to the default factory setting.	
	acs username *username*	
	no acs username	
Parameter Description	**Parameter**	**Description**
	username	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` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
	acs password	Configures the ACS password to be authenticated for the CPE to connect to the ACS.
Platform Description	N/A	

8.4 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**
	seconds	Specifies the delay for backup and restoration of the main program and configuration file of the CPE.
Defaults	N/A	
Command mode	CWMP configuration 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` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#cwmp` `Ruijie(config-cwmp)#no cpe back-up` `Ruijie(config-cwmp)#`	
Related Commands	**Command**	**Description**
	show cwmp configuration	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
Platform Description	N/A	

8.5 cpe inform

	Use this command to configure the periodic notification function of the CPE. Use the **no** form of this command to restore the device to the default factory setting
	cpe inform [**interval** *seconds*] [**starttime** *time*]
	no cpe inform

Parameter Description	**Parameter**	**Description**
	seconds	Specifies the periodical notification interval of the CPE. The value range is from 1 to 3600 in seconds. The default value is 600.
	time	Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.

Defaults	By default, this function is enabled with 600 seconds periodical notification interval.
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 specifies 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` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
Platform Description	N/A	

8.6 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* } **cpe password**	
	no cpe password	
Parameter Description	**Parameter**	**Description**
	password	Configures the CPE user password to be authenticated for the ACS to connect to the CPE.
	encryption-type	Specifies the encryption type, which can be set to **0** (indicating that no encryption is used) or **7** (indicating that simple encryption is used).
	encrypted-password	Specifies the password in encrypted form.
Defaults	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` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
	acs username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Platform Description	N/A

8.7 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 the device to the default factory setting.
	cpe url *url*
	no cpe url

Parameter Description	Parameter	Description
	url	Specifies the URL of the CPE.

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 in http://ip [: port]/ path" format. ● 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 http://10.10.10.1:7547/` `Ruijie(config-cwmp)#`

Related Commands	**Command**	**Description**
	show cwmp configuration	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
Platform Description	N/A	

8.8 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 device to the default factory setting.	
	cpe username *username*	
	no cpe username	
Parameter Description	**Parameter**	**Description**
	username	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` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
	cpe password	Configures the CPE password to be authenticated for the ACS to connect to the

		CPE.
Platform Description	N/A	

8.9 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	CWMP 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` `Enter configuration commands, one per line. End with CNTL/Z.` `Ruijie(config)#no cwmp` `Ruijie(config)#`	
Related Commands	**Command**	**Description**
	show cwmp configuration	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
Platform Description	N/A	

8.10 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 device to the default factory 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		
Configuration Examples	The following example disables the function of downloading main program and configuration files from the ACS `Ruijie#config` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
Platform Description	N/A	

8.11 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 device to the default factory 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	CWMP configuration mode	

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` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.

Platform Description	N/A

8.12 show cwmp configuration

	Use this command to show the current configuration of CWMP.
	show cwmp configuration

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults	N/A
Command mode	privilege EXEC configuration mode
Usage Guide	
Configuration Examples	The following example shows the current configuration of CWMP. `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 pa sword	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	Shows the running status of CWMP.

Platform Description	N/A

8.13 show cwmp status

	Uses this command to check the running status of CWMP
	show cwmp status

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults	N/A
Command mode	CWMP configuration mode
Usage Guide	N/A

Configuration Examples

The following example shows the running status of CWMP.

```
Ruijie(config-cwmp)#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	Shows the current configuration of CWMP.

Platform Description	N/A

8.14 timer cpe-timeout

	Uses this command to configure the session timeout period of the CPE.	
	timer cpe- timeout *seconds*	
	no timer cpe-timeout	
Parameter Description	**Parameter**	**Description**
	seconds	N/A
Defaults	By default, the session timeout period is 30 seconds.	
Command mode	CWMP configuration mode	
Usage Guide	Configures 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 Examples	The following example configures the session timeout period of the CPE to 50 seconds. `Ruijie#config` `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	Shows the current configuration of CWMP.
	show cwmp status	Shows the running status of CWMP.
Platform Description	N/A	

9 Syslog Commands

9.1 clear logging

Use this command to clear the logs from the buffer in privileged EXEC mode.

clear logging

Parameter Description	Parameter	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 Examples	The following example clears the log packets from the memory buffer. `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

9.2 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 Description	Parameter	Description

	ip-address	Sets the IP address of the host receiving log messages.
	vrf-name	Sets the VRF instance connecting with the host.
	ipv6-address	Sets the IPv6 address of the host receiving log messages.
	udp-port *port*	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 Mode	Global configuration 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 Examples	The following example configures a syslog server with IP address 202.101.11.1. `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 Description	N/A	

9.3 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**
	buffer-size	Sets the buffer size, in the range from 4KB to 10MB.
	level	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.

Defaults	The default *buffer-size* is 1MB and *level* 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 insufficent availble continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.

Configuration Examples	The following example allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes. `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 Description	N/A

9.4 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
	level	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 Examples	The following example sets the severity of log that is allowed to be displayed on the console as 6: `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 Description	N/A

9.5 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 Description	Parameter	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

9.6 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 Description	Parameter	Description
	facility-type	Syslog device value. For specific settings, refer to the usage guide.

Defaults	The default is 23 (Local7, 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 Examples

The following example sets the device value of **Syslog** as **kernel**:

```
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

9.7 logging file

	Use this command to save log messages in the log file, which can be saved in expansion 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* | **sd0:***filename* } [*max-file-size*] [*level*]
	no logging file

Parameter Description	**Parameter**	**Description**
	flash	Saves the log file in expansion 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 USB1, This parameter is supported by the device with two USB connectors and the USB extension device.
	filename	Sets the file name. The file type is omitted, which is fixed as txt.
	max-file-size	Sets the maximum file size, in the range from 128K to 6M bytes, The default is 128K,
	level	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 expansion FlASH by default.
Command Mode	Global configuration mode
Usage Guide	You can save log messages in expansion 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 expansion 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 expansion 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

9.8 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	

9.9 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 *seconds*	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 Examples	The following example sets the interval to write log messages into the flash file to 300 seconds. `Ruijie(config)# logging flash interval 300`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

9.10 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 Description	N/A	

9.11 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	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, 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 fitler-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 Examples	The following example sets the filter type to contains-only. `Ruijie(config)# logging filter type contains-only`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

9.12 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	Exact-match filter rule. Fill in all the following three parameters.
	single-match	Single-match filter rule. Fill in one of the following three parameters.
	module *module-name*	Module name.
	mnemonic *mnemonic-name*	Mnemonic name.

	level *level*	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 Description	N/A	

9.13 logging life-time

	Use this command to configure the preservation duration of logs in expansion 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**
	level	Sets the log level, which can be either the level name or the level number.
	days	Sets the preservation duration of logs.
Defaults	No preservation duration is set by default.	

Command Mode	Global configuration mode
Usage Guide	Due to difference in expansion 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 expansion FlASH,
Configuration Examples	The following example sets the preservation duration of logs whose level is 6 to 10 days. `Ruijie(config)# logging life-time level 6 10`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

9.14 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**
	level	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 Examples	The following example sets the severity of log that is allowed to be printed on the VTY window as 6: `Ruijie(config)# logging monitor informational`

Related Commands	**Command**	**Description**
	logging on	Turns on the log switch.
	show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform Description	N/A

9.15 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 fucntion.

logging on

no logging on

Parameter Description	**Parameter**	**Description**
	N/A	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 expansion 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 Examples	The following example disables the log switch on the device. `Ruijie(config)# no logging on`

Related Commands	**Command**	**Description**
	logging buffered	Records the logs to a memory buffer.
	logging server	Sends logs to the Syslog server.
	logging file flash:	Records logs on the expansion 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 Description	N/A

9.16 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 Description	**Parameter**	**Description**
	number	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.
	severity	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 outpt 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	N/A

Description	

9.17 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 Description	Parameter	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, expansion 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

9.18 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 Description	Parameter	Description
	number	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.
	severity	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

9.19 logging server

Use this command to record the logs in the specified Syslog Sever in global configuration mode. Use the **no** form of this command to disable the function.

logging server { *ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* }

no logging server { *ip-address* [**vrf** *vrf-name*] | **ipv6** *ipv6-address* }

Parameter Description	**Parameter**	**Description**
	ip-address	IP address of the host that receives log information.
	vrf-name	Specifies the VRF instance (VPN device forwarding table) connecting to the log host.
	ipv6-address	Specifies IPV6 address for the host receiving the logs.

Defaults	No log is sent to any syslog server by default.
Command	Global configuration mode

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.
Configuration Examples	The following example specifies a syslog server of the address 202.101.11.1: `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

9.20 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**
	interface-type	Interface type.
	interface-number	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 Examples	The following example specifies loopback 0 as the source address of the syslog messages: `Ruijie(config)# logging source interface loopback 0`

Related Commands	**Command**	**Description**
	logging server	Sends logs to the Syslog server.

Platform Description	N/A

9.21 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**
	ip-address	Specifies the source IPV4 address sending the logs to IPV4 log server.
	ipv6-address	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 Examples	The following example specifies 192.168.1.1 as the source address of the syslog messages: `Ruijie(config)# logging source ip 192.168.1.1`

Related Commands	**Command**	**Description**
	logging server	Sends the logs to the Syslog server.

Platform	N/A

Description	

9.22 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 Examples	`Ruijie(config)#line console 0` `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

9.23 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**
	level	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

9.24 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

9.25 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 Mode	Global configuration 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 Examples	The following example enables the logging function to record user operation. `Ruijie(config)# logging user-info command-log`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

9.26 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 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 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 Examples	The following example sets the private syslog format. `Ruijie(config)# service private-syslog`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

9.27 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 Examples	The following example adds serial numbers to the logs. `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

9.28 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 Examples	The following example sets the standard syslog format. `Ruijie(config)# service standard-syslog`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

9.29 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 Examples	The following example adds a system name in the log information: `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

	Command	**Function**
Related Commands	**show logging**	Displays basic configuration of log modules and log information in the buffer.

Platform Description	N/A

9.30 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	**Description**
Parameter Description	*message-type*	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 milisecond 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

9. 31 show logging

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer.

show logging

Parameter Description	**Parameter**	**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:

```
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 %LINEPROTON/A5N/AUPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Ruijie %LINKN/A3N/AUPDOWN: 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

Related Commands	**Command**	**Function**
	logging on	Turns on the log switch.
	clear logging	Clears the log messages in the buffer.

Platform Description	N/A

9.32 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 Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration	The following example displays the outcome of running the **show logging config** command.	

Examples

```
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.

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

9.33 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

9.34 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 Examples	The following example allows log information to be printed on the current VTY window: `Ruijie# terminal monitor`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

Command History	**Version**	**Description**
	N/A	N/A

10 CA-MONITOR Commands

10.1 show power

	Use this command to display power information including that of its basic condition, redundancy, 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 power redundancy mode and check whether power redundancy takes effect and the like. ● 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 Examples	The following example displays the basic power information. 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
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

10.2 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** [{ [[*devid*] *fanid*] **detail** } | **version**]	
Parameter Description	Parameter	Description
	devid	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.
	fanid	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 Examples	The following example displays the fan information in S8605E slave chassis. 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

10.3 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 Examples	The following example displays the temperature and threshold configuration of all boards. 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
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

10.4 power on/off

	Use this command to power on or off the specified board. **power {on | off} [switch** *devid***] slot** *slotid*

Parameter Description	**Parameter**	**Description**
	on	Powers on the specified board.
	off	Powers off the specified board.
	switch *devid*	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 *slotid*	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 Examples	The following example displays switch 2 slot 3 power-off. 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

10.5 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 *devid*	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 *slotid*	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 *seconds*	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	This command is used to power off the specified board, and then automatically power it on. 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	The following example shows slot 3 in the chassis is already upgraded and the upgrade result will be activated by using this command. Ruijie#power cycle slot 3
	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. Ruijie#power cycle slot FE1 interval 600 Slot FE1 power off successfully, and will be on beyond 600 seconds.
Prompt Messages	The board is powered off successfully and will be powered on automatically after 5 seconds. Slot 1/2 power off successfully, and will be on beyond 5 seconds. The board is already powered off and will be powered on automatically after 5 seconds. Slot 1/2 is already off, and will be on beyond 5 seconds. The input slotid is not right. Input slotid(L2) is error. The device does not exit. 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. Operating mistakes cause power-on/off failure. Failed to power cycle slot 1/2 for device error.
Platforms	N/A

10.6 power priority

	Use this command to set the power supply priority of a line card. **power priority [switch** *devid***] 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** *devid***] slot** *slotid*
	Use the **default** form of this command to restore the default setting. **default power priority [switch** *devid***] slot** *slotid*

Parameter Description	**Parameter**	**Description**
	switch *devid*	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 *slotid*	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.
	prio	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	The following example uses slot 3 as a back-up link with lower priority in VSU mode.

Examples	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 Messages	The device does not exist. 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

10.7 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 *level*	speed-level level: 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. Configuring the Operating Mode of Fans	
Configuration Examples	Fans operate in normal mode by default, and thus generate loud noise. 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 Messages	The quiet mode of fans is set successfully. 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. The mode switching fails for the device in the energy-saving mode. Failed to change fan mode, please turn off energy-saving and retry again.
Common Errors	Fail to switch the operating mode for the energy-saving function is enabled. 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

10.8 threshold set temperature

	Use this command to set the temperature threshold for the board. **threshold set temperature [switch** *devid***] {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 *devid*	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.
	temp	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 Mode	Global configuration 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℃ 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℃ 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 Software Authorization Management 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 *filename* 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.
	filename	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.
	target-filename	Specifies the name of the license file.
Command Mode	Global configuration 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(config)#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. 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 Messages	There is not permanent license in the system for backup. `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 Errors	Specify a license file or a file not in the system. 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-peroid** *license days*	
	no license grace-peroid *filename*	
	default license grace-peroid *filename*	
Parameter Description	**Parameter**	**Description**
	filename	The name of the license file for a feature
	days	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	Global configuration 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(config)#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 Messages	The setting is successful. `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.
	filename	Specifies the name of the license file.
Command Mode	Global configuration mode	
Default Level	4	
Usage Guide	The name of the license file can be modified. This command does not require authorization.	

Configuration Examples	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. `Ruijie#show license hostid` `8708EH5F00042` `Ruijie(config)#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 Messages	The specified license file is not in the system. `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 Errors	Specify a license file not on the device. 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 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.
	license	The name of the license file to be removed
	filename	The name of the file to be removed
Command Mode	Global configuration 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 Examples	The following example removes the license file for VSD in the system. `Ruijie(config)#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 Messages	The specified license file is not on the device. (it is named after defd in this example). `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 Errors	The license file has not been installed on the device. 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.

11.5 license unbind

	Use this command to unbind a license. **license unbind** *pak*	
Parameter Description	**Parameter**	**Description**
	pak	Specifies 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 the license on the device before performing unbinding on the Web page. You will get an authenticode after unbinding the license on 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 775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355855.`	

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.
	filename	Specifies the name of the license file.
Command Mode	Global configuration 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(config)#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.	
Configuration Examples	`Ruijie(config)#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 Messages	The specified license file is not in the system. `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 Errors	Install a license file that does not belong to the present device. 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 | file** [*license*] }	
Parameter Description	**Parameter**	**Description**
	all-license	The list of all license files already installed on the device
	file *filename*	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` `Alarm starting point: 120 days before deadline` The following example displays the information of all the license files installed in the system. `Ruijie(config)#show license all-license` `Searching license in the system...` `1. Service name: LIC-FCoE` `Attribute: Permanent, Multiple instance, Releasable` `Installed licenses(s): 123.lic` `2. Service name: LIC-VSD` `Attribute: Temporary, Single instance, Releasable` `Left days: 362` 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

11.8 show license hostid

	Use this command to display the host ID of a license file. **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	The following example displays the host ID of a device.

Examples	Ruijie#show license hostid 1234942570021

11.9 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 details of all PIM ports: `Ruijie#show license usage` `Searching license in the system...` ` 1. Service name: LIC-FCoE` `  Attribute: Permanent, Multiple instance, Releasable` `  Installed licenses(s): 123.lic` ` 2. Service name: LIC-VSD` `  Attribute: Temporary, Single instance, Releasable` `  Left days: 362` 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

11.10 show license unbind-code

	Use this command to display the unbound license code. **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.	

```
Ruijie#show license unbind-code
LICENSE              UNBINDING-CODE
LIC-VSD00000012264933
77571FF68737BFF69FF55FF557F55FF57575B595E58587857FF59FF59765AFF55FF5
LIC-FCOE00000012264966
77571FF68737BFF69FF55FF557F55FF57575B595E5B5B7857FF59FF59765AFF55FF5
LIC-TRILL00000012264988
77571FF68737BFF69FF55FF557F55FF57575B595E5D5D7857FF59FF59765AFF55FF5
```

Field	Description
LICENSE	Unbound license code.
UNBINDING-CODE	Authenticode for license unbinding.

12 Module Hot-plugging/ unplugging Commands

12.1 sysmac

	Use this command to specify a MAC address for the system. Use the **no** form of this command to remove the configuration.	
	sysmac *mac-address*	
	no sysmac	
Parameter Description	Parameter	Description
	mac-address	Clears the MAC address saved in the configuration file.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	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, 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. 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`	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

12.2 remove configuration module slot-num

	Use this command to remove the module configurations.

	remove configuration module *slot-num*	
Parameter Description	**Parameter**	**Description**
	slot-num	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 modue 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	

12.3 remove configuration device device-id

	Use this command to remove the configuration on a VSU device, which validates in VSU mode after restart.	
	remove configuration device *device-id*	
Parameter Description	Parameter	Description
	device-id	The chassis number.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to remove the configuration on a VSU device. It validates after the device is restarted.	

Configuration Examples	The following example clears the configuration on device 1. `Ruijie(config)# remove configuration device 1`

Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

12.4 reset module slot-num

	Use this command to reset a module.
	reset module *slot-num*

Parameter Description	**Parameter**	**Description**
	slot-num	Slot number.

Defaults	N/A
Command Mode	Privileged EXEC 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 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 Examples	The following example displays asset information of the single physical device.	

```
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 Description	N/A	

12.6 **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**
	module-num	(Optional) Module number.

Defaults	N/A
Command Mode	Privileged EXEC mode.
Usage Guide	Use this command to display details of the module
Configuration Examples	`Ruijie# show version module detail 2` `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	Displays slot details.
Platform Description	N/A	

12.7 show version slots [*slot-num*]

	Use this command to display the details of the slot.
	show version slots [*slot-num*]

Parameter Description	**Parameter**	**Description**
	num	(Optional) Slot number.
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	Displays the details of the module.
Platform Description	N/A	

13 Supervisor Module Redundancy Commands

13.1 auto-sync time-period

	Use this command to configure the auto-sync time-period of runing-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**
	value	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 Examples	The following example enters redundancy configuration mode. `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 master/slave 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 master supervisor module, the module will be reset and the slave supervisor module will act as a master supervisor module. The following conditions are required to perform hot backup switchover: ● This command is executed on the master supervisor module. There is a slave supervisor module. ● Hot backups on all virtual switch devices (VSDs) are in real-time status. ● Hot backup switchovers on VSDs are not prevented temporarily by any service entity. When there are multiple VSDs, the system judges whether the hot backup on each VSD allows master/slave switchover; If any VSD does not allow the switchover, the command fails. Otherwise, master/slave switchovers are enforced on all VSDs.
Configuration Examples	The following example performs master/slave supervisor module switchover. `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 master supervisor module.
Platform Description	N/A	

13.4 redundancy reload

	Use this command to reset the supervisor module.
	redundancy reload { **peer** | **shelf** [*switchid*] }

Parameter Description	**Parameter**	**Description**
	peer	Resets the slave supervisor module.
	shelf	Resets both the master and slave 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.
	switchid	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 Examples	The following example resets the slave supervisor module. `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 Description	N/A	

13.5 show redundancy states

	Use this command to display the current redundancy states.
	show redundancy states

Parameter Description	**Parameter**	**Description**
	states	Displays the redundancy status of the master or the slave devices.
Defaults	N/A	
Command Mode	User EXEC mode / Privileged EXEC mode	

Usage Guide	Currently, only 1:1 hot backup (for the global master board and slave board) is supported in the VSU mode. Therefore, only the hot backup state of the local and peer device is displayed.
Configuration Examples	The following example displays the redundancy states of master/slave supervisor modules. `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 slave 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 master 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/SD 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 Examples	The following example displays the information about the USB device:

```
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 Description	N/A	

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 Description	N/A	

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 Description	**Parameter**	**Description**
	int	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 Examples	The following example enables LLDP two-event classification. `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 Examples	The following example disables the PoE function on port GigabitEthernet 0/1, `Ruijie(config)# interface GigabitEthernet 0/1` `Ruijie(config-if-GigabitEthernet 0/1)# no poe enable`	

Related Commands	**Command** / **Description**
	N/A / N/A
Platform Description	N/A

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**
	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	This function is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A
Configuration Examples	The following example disables PoE for line card 2. `Ruijie# configure` `Ruijie(config)# no poe enable pse slot 2`
Related Commands	**Command** / **Description**
	N/A / N/A
Platform Description	N/A

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**
	int / 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.
Defaults	The maximum power is not set by default.	
Command Mode	Interface configuration mode	
Usage Guide	N/A.	
Configuration Examples	The following example sets the maximum power for port GigabitEthernet 0/1 to 20W. `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 Description	N/A	

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**
	max-power	The maximum power, in the range from 0 to 1440W.
	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 *max-power* is 369.6W for the 24-port line card and 739.2W for the 48-port line card.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

Configuration Examples	The following example sets the maximum PoE power for line card 2 to 300W. `Ruijie(config)# poe max-power 300 pse slot 2`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

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**}
	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,
Defaults	The default mode is auto.
Command Mode	Global configuration mode
Usage Guide	N/A
Configuration Examples	The following example sets the PoE management mode to energy-saving mode. `Ruijie# configure` `Ruijie(config)# poe mode energy-saving` `Ruijie(config)# end`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

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**
	pd-name	PD descriptor name, a string no more than 32 characters.

Defaults	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A
Configuration Examples	The following example sets the PD descriptor for port GigabitEthernet 0/1. `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 Description	N/A	

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**
	name	Time-range name.
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the port GigabitEthernet 0/1 to be disabled from 8:30 to 17:30 every day. `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 Description	N/A	

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 Examples	The following example sets the PoE priority for port GigabitEthernet 0/1 to critical. 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 Description	N/A	

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	**Parameter**	**Description**
	int	Reserve power percentage, in the range from 0 to 50.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the reserve power for the system to 10%. `Ruijie(config)# poe reserve-power 10` `Ruijie(config)# end`	
Related Commands	**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	**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	The following example enables uninterruptible PoE for warm start and saves configuration. `Ruijie(config)# poe uninterruptible-power` `Ruijie(config)# end` `Ruijie#write`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

15.16 poe warning-power

	Use this command to set the power alarm threshold for the system. Use the **no** or **default f**orm of this command to restore the default setting,
	poe warning-power *int*
	no poe warning-power
	default poe warning-power
Parameter Description	**Parameter** / **Description** *int* / 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 waring-power 80` `Ruijie(config)# end` `Ruijie#write`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

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**
	interface-name	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.	

```
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
```

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 Mode	Privileged EXEC mode	
Usage Guide	This command is used to display PoE status or configuration of all ports.	
Configuration Examples	The following example displays PoE status of all ports.	

```
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  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 Description	N/A

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 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	**Command**	**Description**

Commands		
	N/A	N/A
Platform Description	N/A	

16 UFT Commands

16.1 switch-mode mode_type slot slod_number

	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**
	mode_type	Indicates the UFT operating mode. In stand-alone mode, the line card can operate in the following modes: ● **Default:** Default mode, which is applied to most of application scenarios. ● **bridge:** Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate. ● **gateway:** Gateway mode, which is applied to the application scenario in which Layer 3 services dominate. ● **gateway-max:** Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed. ● **gateway-ndmax:** Gateway-ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed. ● **label:** Label mode, which is applied to the application scenarios that require a great amount of MPLS labels. ● **route-v4max:** IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes. ● **route-v6max:** IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.
	slot_num	Indicates the corresponding line card installed in the chassis.
Defaults	The Default UFT operating mode is **Default**.	
Command	Global configuration mode	

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)` `!` `cwmp` `!` `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

16.2 switch-mode mode_type switch switch_id slot slod_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**
	mode_type	Indicates the UFT operating mode. In VSU mode, the line card can operate in the following modes: ● **Default**: Default mode, which is applied to most of application scenarios. ● **bridge**: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate. ● **gateway**: Gateway mode, which is applied to the application scenarios in which Layer 3 services dominate. ● **gateway-max**: Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed. ● **gateway-ndmax**: Gateway_ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed. ● **label**: Label mode, which is applied to the application scenarios that require a great amount of MPLS labels. ● **route-v4max**: IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes. ● **route-v6max**: IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.
	switch_num	Indicates the chassis or box device number in VSU mode.
	slot_num	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)` `!` `cwmp` `!` `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

16.3 show switch-mode status

	Use this command to display the UFT mode of a switch. **show switch-mode status**

<table>
<tr><td>Parameter Description</td><td>Parameter</td><td>Description</td></tr>
<tr><td></td><td>N/A</td><td>N/A</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Command Mode</td><td colspan="2">Privileged EXEC mode, global configuration mode, interface configuration mode</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Default Level</td><td colspan="2">14</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Usage Guide</td><td colspan="2">N/A</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Configuration Examples</td><td colspan="2">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:
<table><tr><td>Field</td><td>Description</td></tr><tr><td>Slot No</td><td>Displays only slot No. in stand-alone mode; displays both device No. and slot No. in VSU mode.</td></tr><tr><td>Switch-Mode</td><td>Indicates the UFT operating mode.</td></tr></table></td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Prompt Messages</td><td colspan="2">N/A</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td>Platforms</td><td colspan="2">N/A</td></tr>
</table>

17 Package Management Commands

17.1 clear storage

	Use this command to remove an installation package on the local device. **clear storage** [*url*]

Parameter Description	**Parameter**	**Description**
	url	A local *url* directory or full pathname 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	`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#`
Verification	Check specified *url*
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 *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.
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	The following example activates a patch on the box device. `Ruijie#patch active` ` Active the patch package success` The following example activates a patch on the chassis device. `Ruijie#patch active slot 8` `[Slot 8]:` ` Active the patch package success`	
Verification	Use the **show patch** command to display patch information.	
Prompt Messages	The patch is activated successfully. `Active 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 activated or running status. `The patch status is already active or running` Contact the service center to solve the package problem. `Cannot find the package's scripts file`	
Common Errors	There is no hot patch installed on current device. The hot patch on current device is already activated.	
Platforms	N/A	

17.3 patch deactive

	Use this command to deactivate a patch. **patch deactive** [**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 can be performed to deactivate a patch only after the patch is in the activated status.	
Configuration Examples	The following example deactivates a patch on the box device. `Ruijie#patch deactive` ` Deactive the patch package success` The following example deactivates a patch on the chassis device. `Ruijie#patch deactive slot 8` ` [Slot 8]:` `Deactive the patch package success`	
Verification	Use the **show patch** command to display patch information.	
Prompt Messages	The patch is deactivated successfully. `Deactive 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 Errors	There is no hot patch installed on current device. 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 Examples	The following example removes the installed hot patch package from the box device. `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 Messages	The patch is uninstalled successfully. `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 *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	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 Messages	The patch is activated permanently. `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 Errors	There is no hot patch on current device. 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 *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.
	component _name	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 Mode	Privileged EXEC 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.

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 component bridge
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 Messages	The execution is successful with all components information displayed. `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.
	patch _name	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 Mode	Privileged EXEC mode	
Default Level	2	

Usage Guide	This command is used to check all patches already installed on the device and their information.
Configuration Examples	The following example displays all patches already installed on the box device.

```
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 component bridge
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 Messages	The information of the patch is displayed after successful running. 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 Messages	The auto-sync information of the system is displayed after running. 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 history

	Use this command to display the upgrade history. **show upgrade history**	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Command Mode	Privileged EXEC mode	
Default Level	2	
Configuration Examples	The following example displays the upgrade history. `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	

17.10 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	This command is supported only on the chassis device.

17.11 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**
	url	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 Examples	The following example upgrades the main package on the device. `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:/ca-octeon_11.0(1B2)_20131106_main_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 Messages	The prompt message of successful running is displayed. `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

17.12 upgrade auto

	Use this command to upgrade an installation package automatically without interrupting the service. **upgrade auto** *url* [**force**]	
Parameter Description	**Parameter**	**Description**
	url	The local path indicates where an installation package is stored.
	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 (use 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 Examples	The following example upgrades the main package automatically without interrupting the service. 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.

17.13 upgrade auto-sync package

	Use this command to check the range for the auto-sync upgrade of the system on the device. **upgrade auto-sync package** *url*	
Parameter Description	**Parameter**	**Description**
	url	The path for package upgrade during automatic system upgrade.
Defaults	It is the path of upgrade package where the last system upgrade is performed.	
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	It is recommended to use default system configuration.	
Configuration Examples	The following example sets the path to the upgrade package in the USB flash disk. `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 visited.	

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`

17.14 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	Judges whether to perform 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. `Ruijie# upgrade auto-sync policy coordinate`	
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. `Upgrade auto-sync policy is set as coordinate.`	

17.15 upgrade auto-sync range

	Use this command to set the range of auto-sync upgrade. **upgrade auto-sync range** [**chassis** | **vsu**]	
Parameter	**Parameter**	**Description**

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. `Ruijie# upgrade auto-sync range vsu`	
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. `Upgrade auto-sync range is set as vsu.`	

17.16 upgrade download tftp

	Use this command to download, install and upgrade installation packages on the tftp server. **upgrade download tftp:/***path*	
Parameter Description	**Parameter**	**Description**
	path	The path of installation packages on the tftp server This command is downloaded and upgraded automatically from the server.
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 Examples	The following example upgrades the main package. `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 Messages	The prompt message of successful running is displayed. `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`

17.17 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 err or 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*] [**aux**] **interface**[*interface-id*]
	Use the **no** form of this command to disable OpenFlow. **no of controller-ip** [*ip-address*]

Parameter Description	**Parameter**	**Description**
	ip-address	Controller IP address. If you configure the **no** form of this command without any parameter, all controllers are disabled. (OpenFlow1.3 supports connection to multiple controllers and OpenFlow1.0 supports connection to one single controller).
	port *port-id*	Controller access port ID. The default for OpenFlow1.0 is 6633 and for OpenFlow1.3 is 6653.
	aux	Auxiliary switch (it takes effect for only OpenFlow1.3)
	Interface *interface-id*	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 Level	N/A
Usage Guide	N/A
Configuration Examples	The following example enables OpenFlow. `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 stp

	Use this command to enable/disable STP function for the SDN controller. [**no**] **of stp**

Parameter Description	**Parameter**	**Description**
	N/A	N/A
Command	Global configuration mode	

Mode	
Default Level	This function is disabled for SDN controller by default.
Usage Guide	Use this command to enable/disable STP function for the SDN controller. This command takes effect only after enabling the OpenFlow function.
Configuration Examples	The following example enables STP. `Ruijie(config)#no of stp` The following example disables STP. `Ruijie(config)#of stp`

18.3 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 Level	N/A	
Usage Guide	Use this command to display the OpenFlow version on the device.	
Configuration Examples	The following example displays the connection between the current device and the controller. `Ruijie#show of`	

18.4 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 Level	N/A	

Usage Guide	Running the **of controller-ip** command before configuring this command. Otherwise, the flow table entries are not displayed.
Configuration Examples	The following example display flow table entries. `Ruijie#show of flowtable`

18.5 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 Level	N/A	
Usage Guide	Running the **of controller-ip** command before configuring this command. Otherwise, the port information is not displayed.	
Configuration Examples	The following example displays port information of OpenFlow device. `Ruijie#show of port`	

Ethernet Switching 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
kilobits	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 [*seconds*]

no carrier-delay

Parameter Description

Parameter	Description
seconds	Optional parameter in the range from 1 to 60 in the unit of seconds.

Defaults The default is 2.

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. 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
```

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
interface-id	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
interface-id	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 Examples The following example resets the interface gigabitethernet 1/1.

```
Ruijie# clear interface gigabitethernet 1/1
```

Related Commands

Command	Description
shutdown	Disables the interface.

Platform Description N/A

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
string	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 Examples The following example configures the alias of interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# description GBIC-1
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

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 Mode Interface configuration mode.

Usage Guide The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

Configuration Examples The following example specifies the duplex mode for the interface.

```
Ruijie(config-if)# duplex full
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.7 errdisable recovery

Use this command to recover the interface in violation.

errdisable recovery [**interval** *time*]

Parameter Description

Parameter	Description
time	Time for the command to take effect. The range is from 30 to 86,400 seconds.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide Use the command to recover the port that triggers violation after being configured with the **violation shutdown** command.

Configuration Examples The following example recovers the violation interface gigabitethernet 1/1.

```
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 Description N/A.

1.8 fiber antifake ignore

Use this command to disable the anti-fraud check function. Use the **no** form of this command to restore the default setting.

fiber antifake ignore

no fiber antifake ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide The anti-fraud check function is enabled by default. When a non-original optical module is inserted, alarm logs are printed. If you disable this function, alarm logs are not printed.

Configuration Examples The following example disables the anti- fraud check function.

```
Ruijie(config)# fiber antifake ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.9 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 Mode Interface configuration mode.

Usage Guide Use the **show interfaces** command to display the flow control configuration.

Configuration Examples This example enables flow control on fastEthernet port 1/1.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# flowcontrol on
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.10 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 Mode Interface configuration mode

Usage Guide In general, the auto-negotiation status is determined by interface speed, duplex, flow control and auto-negotiation factor mode.

Configuration Examples The following example enables auto-negotiation mode on interface GigabitEthernet 1/1.

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# negotiation mode on
```

Related Commands

Command	Description
N/A	N/A

Platform Description

For the 10 Gigabit fiber port, the auto-negotiation function is disabled forever, that is, the status of auto-negotiation is OFF forever.

When you insert the optical transceiver into the 40 Gigabit fiber port, the auto-negotiation is disabled; when the copper cable is inserted, the auto-negotiation is enabled.

1.11 interface

Use this command to enter the interface configuration mode.

interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type	The interface type.
interface-number	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 Description N/A

1.12 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
port-range	The interface type and ID range, entered in the form of *interface-type slot-number/interface-number*. The interface can be either an Ethernet physical interface or a loopback interface.
macro *macro_name*	The macro name which represents the interface range.

Defaults The **interface range** command is disabled by default.

Command Mode Global configuration 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 route1 gigabitEthernet 0/0-2
Ruijie(config)# interface range macro route1
Ruijie(config-if-range)# bandwidth 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.13 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

1.14 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
seconds	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 Description N/A

1.15 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 Examples 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 Description N/A

1.16 mtu

Use this command to set the MTU supported on the interface.

mtu *num*

Parameter Description

Parameter	Description

num	64 to 9216 (or 65536, which varies by products)

Defaults The default is 1500.

Command Mode Interface configuration mode.

Usage Guide This command is used to set the maximum transmission unit (MTU) supported on the interface.

Configuration Examples The following example sets the MTU supported on interface gigabitethernet 1/1 to 9216.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mtu 9216
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description The MTU configuration applies on both the ingress port and the egress port.
N/A

1.17 parallel detect disable

Use this command to disable the parallel detect function.
parallel detect disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide Parallel detection is operational after enabled whatever the negotiation mode is.

Configuration Examples The following example disables the parallel detection function on GigabitEthernet 0/1.

```
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# parallel detect disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.18 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 Mode Global configuration 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 Examples The following example enables oscillation protection on the port.

```
Ruijie(config)# physical-port dither protect
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.19 protected-ports route-deny

Use this command to block L3 routing between 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 blocks L3 routing between protected ports.

```
Ruijie(config)# protected-ports route-deny
```

Related Commands

Command	Description
show running-config	Displays the protected ports route-deny configuration.

Platform Description N/A

1.20 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 N/A

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

1.21 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

1.22 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 Examples The following example enables the interface index persistence.

```
Ruijie(config)# snmp-server if-index persist
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.23 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 | 10G | 40G | 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.
10G	The transmission rate of the interface is 10Gbps.
40G	The transmission rate of the interface is 40Gbps.
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 Examples The following example sets the speed on interface gigabitethernet 1/1 to 100Mbps.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# speed 100
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.24 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 Mode Interface configuration 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 Examples The following example configures a Layer 3 interface.

```
Ruijie(config-if)# switchport
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.25 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 Description

Parameter	Description
vlan-id	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.

```
Ruijie(config)# interface gigabitethernet 1/1
```

```
Ruijie(config-if)# switchport access vlan 2
```

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

1.26 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 Mode Interface configuration 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 Examples The following example specifies a L2 interface (switch port) mode.

```
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 Description N/A

1.27 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 Mode Interface configuration 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 Examples The following example configures interface gigabitethernet 1/1 as a protected port.

```
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)# switchport protected
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.28 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 *vlan-list*	Configures the list of VLANs allowed on the trunk port. *vlan-list* 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 *vlan-id*	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 Examples The following example removes port 1/15 from VLAN 2.

```
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

1.29 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
	interface-id interface-number	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.
The functions of showing the optical module information, alarming the fault and diagnosing the parameters shall be used combining with the optical module of the RG network.
To show the optical module and alarm the fault and diagnose the parameters, the function of Digital Diagnostic Monitoring must be supported by the optical module.

Configuration Examples The following example displays the interface information when the Gi0/1 is a Trunk 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: 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
```

The following example displays the MTU information on the interface GigabitEthernet 1/1.

```
Ruijie#show interfaces GigabitEthernet 1/1 mtu
interface              MTU
-------------------   -------
GigabitEthernet 1/1    1500
```

The following example displays the bandwidth usage on the interface GigabitEthernet 1/1.

```
Ruijie#show interfaces GigabitEthernet 1/1 usage
Interface             Bandwidth         Bandwidth Usage
-------------------   ---------------   ----------------
GigabitEthernet 1/1   1,000,000 Kbit     20%
```

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 Description N/A

1.30 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**]

Parameter Description

Parameter	Description
interface-type interface-number	(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.

Defaults N/A

Command Mode All CLI user modes

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
```

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
```

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
```

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
```

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

1.31 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
interface-type interface-number	The interface type and ID.

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 Examples The following example displays the link state statistics of interface GigabitEthernet 0/1.

```
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 Description N/A

1.32 show interfaces status

Use this command to display interface status information.

show interfaces [*interface-type interface-number*] **status**

Parameter Description

Parameter	Description
interface-type interface-number	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.

```
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 Description N/A

1.33 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
interface-type interface-number	(Optional) The interface type and ID.

Defaults

Command Mode All CLI user modes

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 Description N/A

1.34 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
interface-type interface-number	The interface type and ID.
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 Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the transceiver information of all interfaces is displayed.

Configuration Examples The following example displays the transceiver information of interface Gigabitethernet 5/4.

```
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

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

1.35 show interfaces usage

Use this command to display bandwidth usage of the interface.

show interfaces [*interface-type interface-number*] **usage**

Parameter Description	Parameter	Description
	interface-type interface-number	(Optional) The interface type and ID.

Defaults N/A

Command Mode All CLI user modes

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    Bandwidth Usage
-------------------------------- ------------- ------------------
GigabitEthernet 0/0            1000000  Kbit 0.001840950%
```

Bandwidth refers to the interface link bandwidth, the maximum speed of link.

Related Commands	Command	Description
	N/A	N/A

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*]

Parameter Description

Parameter	Description
dynamic	Clears all the dynamic MAC addresses.
address *mac-addr*	Clears the specified dynamic MAC address.
interface *interface-id*	Clears all the dynamic MAC addresses of the specified interface.
vlan *vlan-id*	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 Description N/A

2.2 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.

```
Ruijie(config)# mac-address-learning disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 mac-address-learning

Use this command to enable the port address learning. Use the **no** form of this command to restore the default setting.

mac-address-learning

no mac-address-learning

Parameter Description

Parameter	Description
N/A	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.

```
Ruijie(config-if)# no mac-address-learning
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.4 mac-address-table aging-time

Use this command to specify the aging time of the dynamic MAC address. Use the **no** form of the command to restore the default setting.

mac-address-table aging-time *seconds*

no mac-address-table aging-time

Parameter Description	Parameter	Description
	seconds	Aging time of the dynamic MAC address (in seconds). The time range depends on the switch.

Defaults The default is 300.

Command Mode Global configuration mode.

Usage Guide Use **show mac-address-table** aging-time to display configuration.

Use **show mac-address-table dynamic** to display the dynamic MAC address table.

Configuration Examples The following example sets the aging time of the dynamic MAC address to 150 seconds.

```
Ruijie(config)# mac-address-table aging-time 150
```

Related Commands	Command	Description
	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 Description N/A

2.5 mac-address-table filtering

Use this command to configure the filtering MAC address. Use the **no** 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*

Parameter Description

Parameter	Description
mac-address	Filtering Address
vlan-id	VLAN ID, in the range from 1 to 4094.

Defaults No filtering address is configured by default.
When configuring this command without the **source** or **destination** specified, the frame received in the specified VLAN, which has the same source/destination MAC address with the specified MAC address, will be filtered.

Command Mode Global configuration mode.

Usage Guide The filtering MAC address shall not be a multicast address. Use the **show mac-address-table filtering** command to display the filtering MAC addresses.

Configuration Examples The following example configures the filtering MAC address for VLAN 1.

```
Ruijie(config)# mac-address-table filtering 00d0f8000000 vlan 1
```

Related Commands

Command	Description
clear mac-address-table filtering	Clears the filtering MAC address.

Platform Description N/A

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 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 logging for MAC-flapping among different ports within a VLAN.

Configuration Examples The following example enables MAC-flapping logging.

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table flapping-logging
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.7 mac-address-table notification

Use this command to enable the MAC address notification function. Use The **no** 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**]

Parameter Description	Parameter	Description
	interval *value*	Sets the interval of sending the MAC address trap message, 1 second by default.
	history-size *value*	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 Description N/A

2.8 mac-address-table static

Use this command to configure a static MAC address. Use the **no** 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*

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the specified entry
vlan-id	VLAN ID of the specified entry, in the range from 1 to 4094.
interface-id	Interface (physical interface or aggregate port) that packets are forwarded to

Defaults No static MAC address is configured by default.

Command Mode Global configuration 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 Examples The following example configures a static MAC address.

```
Ruijie(config)# mac-address-table static 00d0.f800.073c vlan 4 interface gigabitethernet 1/1
```

Related Commands

Command	Description
show mac-address-table static	Displays the static MAC address.

Platform Description N/A

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 Description

Parameter	Description
num	Sets the maximum number of MAC addresses.

Defaults The maximum number is not set by default.

Command Mode VLAN configuration mode / Interface configuration 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 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
```

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 Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 show mac-address-learning

Use this command to display the MAC address learning.

show mac-address-learning

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 MAC address learning.

```
Ruijie# show mac-address-learning
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.11 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 *mac-addr*	The MAC address.
	interface *interface-id*	The Interface ID.
	vlan *vlan-id*	The VLAN ID, in the range from 1 to 4094.

Defaults N/A

Command Mode All modes

Usage Guide In the Type column, STATIC represents static address, DYNAMIC represents dynamic address, FILTER represents filter address and OTHER represents successfully authenticated address (including 1x authentication, MAB authentication and WEB authentication).

Configuration Examples The following example displays the MAC address.

```
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 Description N/A

2.12 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 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 aging time of the dynamic MAC address.

```
Ruijie# show mac-address-table aging-time
Aging time  : 300
```

Related

Command	Description

Commands	mac-address-table aging-time	Sets the aging time of the dynamic MAC address.

Platform Description N/A

2.13 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 Description

Parameter	Description
interface *interface-id*	Interface ID
vlan *vlan-id*	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 Examples The following example displays the number of MAC address entries.

```
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: 8139The 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 Description N/A

2.14 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

show mac-address-table dynamic [**address** *mac-add r*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN of the entry, in the range from 1 to 4094.
interface-id	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 Description N/A

2.15 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 Description	Parameter	Description
	mac-addr	Destination MAC address of the entry
	vlan-id	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 Description N/A

2.16 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	Displays the dynamic MAC address learned on all VLANs which are configured with the maximum number of dynamic MAC address learning.
vlan-id	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.
interface-id	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 Description N/A

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 Description

Parameter	Description
interface-id	Displays the MAC address information of the specified Interface (physical interface or aggregate port).
vlan-id	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 all the MAC addresses on interface gigabitethernet 1/1.

```
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	Displays the static MAC address.
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 Description N/A

2.18 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 *interface-id*	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 Description N/A

2.19 show mac-address-table static

Use this command to display the static MAC address.

show mac-address-table static [**addr** *mac-add r*] [**interface** *interface-Id*] [**vlan** *vlan-id*]

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry, within the range from 1 to 4094.
interface-id	Interface of the entry physical interface or aggregate port

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the static MAC addresses

```
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 Description N/A

2.20 show mac-address-table vlan

Use this command to display all addresses of the specified VLAN.

show mac-address-table vlan [*vlan-id*]

Parameter Description

Parameter	Description
vlan-id	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.

```
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 Description N/A

2.21 snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. Use The **no** form of the command to restore the default setting.

snmp trap mac-notification { **added** | **removed** }

no snmp trap mac-notification { **added** | **removed** }

Parameter Description

Parameter	Description
added	Notifies when a MAC address is added.
removed	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 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 Description

Parameter	Description
capacity-mode	Configures the capacity mode.

Defaults The default *capacity-mode* varies with the device.

Command Mode Global configuration mode

Usage Guide N/A

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 Description N/A

3.2 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 | src- l4port | dst-l4port | src-dst-l4port | src-ip-src-l4port | src-ip-dst-l4port | dst-ip-src-l4port | dst-ip-dst-l4port | src-ip-src-dst-l4port | dst-ip-src-dst-l4port | src-dst-ip-src-l4port | src-dst-ip-dst-l4port | src-dst-ip-src-dst-l4port | round-robin}

no aggregateport load-balance

Parameter Description

Parameter	Description
dst-mac	Traffic is distributed according to 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	Traffic is distributed according to 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	Traffic is distributed according to 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	Traffic is distributed according to 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	Traffic is distributed according to 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	Traffic is distributed according to 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/src-dst-ip-src-dst-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
src- l4port	Load balance based on the L4 source port number.
dst- l4port	Load balance based on the L4 destination port number.
src-dst-l4port	Load balance based on the L4 source port number and L4 destination port number.
src-ip-src-l4port	Load balance based on the source IP address and the L4 source port number.
src-ip-dst-l4port	Load balance based on the source IP address and the L4 destination port number.
dst-ip-src-l4port	Load balance based on the destination IP address and the L4 source port number.
dst-ip-dst-l4port	Load balance based on the destination IP address and the L4 destination port number.
src-ip-src-dst	Load balance based on the source IP address, L4 source port number and L4

-l4port	destination port number.
dst-ip-src-dst -l4port	Load balance based on the destination IP address, L4 source port number and L4 destination port number.
src-dst-ip-src -l4port	Load balance based on the source IP address, the destination IP address and L4 source port number.
src-dst-ip-dst -l4port	Load balance based on the source IP address, the destination IP address and L4 destination port number.
round-robin	Load balance based on round robin.

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 Use the **show aggregateport** command to display load-balance configuration.

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 Description For S7800E-ED/DB products, if you perform load balancing based on the source MAC address, the destination MAC address, or the combination of the source MAC address and the destination MAC address, the device takes fields of Ethernet type and VLAN as equivalence factors by default.
For S7800E-ED/DB products, in the non-enhanced mode, load balancing of IGMP Snooping and multicast packets is based on t src-ip, dst-ip or src-ip+dst-ip; traffic balancing of unknown unicast packets, multicast packets and broadcast packets is based on src-mac, dst-mac or src-mac+dst-mac. But a L3 packet (unknown unicast packets, unknown multicast packets and unknown broadcast packets) cannot achieve load balancing based on src-ip or dst-ip on a L2 port. However, the enhanced mode can address this problem with load balancing based on the packet type.
In the src-dst-ip-l4port mode, modification to the L4port affects the traffic balancing of unicast packets on S7800E-ED/DB products.
S7800E-ED/DB products support aggregate-port-based load balancing. The aggregate-port-based load balancing configuration supports SMAC, DMAC, SMAC+DMAC, SIP, DIP or SIP+DIP.
S7800E-ED/DB products support configuration of the following enhanced traffic balancing templates:
L2 template: src-mac dst-mac vlan l2-protocol src-port
IPv4 template: src-ip dst-ip protocol vlan l4-src-port l4-dst-port src-port
IPv6 template: src-ip dst-ip protocol vlan l4-src-port l4-dst-port src-port
MPLS template::top-label 2nd-label vlan src-ip dst-ip src-port
TRILL template: src-mac dst-mac vlan
FCOE template: src-id dst-id ox-id
For S7800E-ED/DB products, if the enhanced MPLS template contains the VLAN field, the balancing

algorithm takes effect only when the ingress packet is a tagged MPLS packet and the action is popping the tag.

3.3 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 Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function cannot be enabled by running the **snmp trap link-status** command in interface configuration mode.

Configuration Examples The following example enables the LinkTrap function on the aggregate port members.

```
Ruijie# configure terminal
Ruijie(config)# aggregateport member linktrap
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.4 fcoe field

Use this command to set the load balance mode for FCOE packets in the enhanced template. Use the **no** form of this command to restore the default setting.

fcoe field [**src-id**] [**dst-id**] [**ox-id**]

no fcoe field

Parameter Description

Parameter	Description
src-id	Load balance based on the source ID.
dst-id	Load balance based on the destination ID.
ox-id	Load balance based on the Originator Exchange ID.

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

3.5 interface 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.

interface aggregateport *ap-number*

no interface aggregateport *ap-number*

Parameter Description

Parameter	Description
ap-number	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 This example creates AP 5 and enters its interface configuration mode.

```
Ruijie# configure terminal
Ruijie(config)# interface aggregateport 5
```

```
Ruijie(config-if-Aggregateport 5)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 ipv4 field

Use this command to configure the load balance mode of IPv4 packets in a specified load balance enhanced 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**] [**dst-port**]

no ipv4 field

Parameter Description

Parameter	Description
src-ip	Traffic is distributed according to the source IP addresses of the incoming IPv4 packets.
dst-ip	Traffic is distributed according to the destination IP addresses of the incoming IPv4 packets.
protocol	Traffic is distributed according to the protocol types of the incoming IPv4 packets.
l4-src-port	Traffic is distributed according to the L4 source port numbers of the incoming IPv4 packets.
l4-dst-port	Traffic is distributed according to the L4 destination port numbers of the incoming IPv4 packets.
vlan	Traffic is distributed according to the VLANs of the incoming IPv4 packets.
src-port	Traffic is distributed according to the source port numbers of the incoming IPv4 packets.
dst-port	Traffic is distributed according to the destination port numbers of the incoming IPv4 packets.

Defaults The default load balance mode is **src-ip** and **dst-ip**.

Command Mode Load balance enhanced profile configuration mode.

Usage Guide Use the **show load-balance-profile** command to display the load balance mode configuration.

Configuration Examples The following example sets the load balance mode of IPv4 packets to **src-ip**.

```
Ruijie(config-load-balance-profile)# ipv4 field src-ip
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

3.7 ipv6 field

Use this command to configure the load balance mode of IPv6 packets in a specified load balance enhanced profile. Use the **no** form of this command to restore the default setting.

ipv6 field [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**vlan**] [**src-port**] [**dst-port**]

no ipv6 field

Parameter Description

Parameter	Description
src-ip	Traffic is distributed according to the source IP addresses of the incoming IPv6 packets.
dst-ip	Traffic is distributed according to the destination IP addresses of the incoming IPv6 packets.
protocol	Traffic is distributed according to the protocol types of the incoming IPv6 packets.
l4-src-port	Traffic is distributed according to the L4 source port numbers of the incoming IPv6 packets.
l4-dst-port	Traffic is distributed according to the L4 destination port numbers of the incoming IPv6 packets.
vlan	Traffic is distributed according to the VLANs of the incoming IPv6 packets.
src-port	Traffic is distributed according to the source port numbers of the incoming IPv6 packets.
dst-port	Traffic is distributed according to the destination port numbers of the incoming IPv4 packets.

Defaults The default load balance mode is **src-ip** and **dst-ip**.

Command Mode Load balance enhanced profile configuration mode.

Usage Guide Use the **show load-balance-profile** command to display the load balance mode configuration.

Configuration Examples The following example sets the load balance mode of IPv6 packets to **src-ip**.

```
Ruijie(config-load-balance-profile)# ipv6 field src-ip
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.8 l2 field

Use this command to configure the load balance mode of L2 packets in a specified load balance enhanced profile. Use the **no** form of this command to restore the default setting.

l2 field [**src-mac**] [**dst-mac**] [**l2-protocol**] [**vlan**] [**src-port**]

no l2 field

Parameter Description	Parameter	Description
	src-mac	Traffic is distributed according to the source MAC addresses of the incoming L2 packets.
	dst-mac	Traffic is distributed according to the destination MAC addresses of the incoming L2 packets.
	l2-protocol	Traffic is distributed according to the L2 protocol types of the incoming L2 packets.
	vlan	Traffic is distributed according to the VLANs of the incoming L2 packets.
	src-port	Traffic is distributed according to the source port numbers of the incoming L2 packets.

Defaults The default load balance mode is **src-mac**, **dst-mac**, and **vlan**.

Command Mode Load balance enhanced profile configuration mode.

Usage Guide Use the **show load-balance-profile** command to display the load balance mode configuration.

Configuration Examples The following example sets the load balance mode of L2 packets to **src-mac** and **src-prot**.

```
Ruijie(config-load-balance-profile)# l2 field src-mac src-port
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.9 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
port-priority	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 Examples This example sets the LACP port priority of interface Gi0/1 to 4096.

```
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 Description N/A

3.10 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 Interface configuration mode

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.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lacp short-timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.11 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
system-priority	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 Examples The following example sets the LACP system priority to 4096.

```
Ruijie(config)# lacp system-priority 4096
```

Related Commands	Command	Description
	port-group *key* **mode** { **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 Description N/A

3.12 load-balance-profile

Use this command to create a load balance enhanced profile and apply the profile. Use the **no** form of this command to restore the default setting.

load-balance-profile *profile-name*

no load-balance-profile *profile-name*

Parameter Description	Parameter	Description
	profile-name	Specifies the profile name, which contains up to 31 characters.

Defaults No enhanced template is created by default.

Command Mode Global configuration mode.

Usage Guide This command supports only one profile. Use the **show load-balance-profile** command to display the current configuration.

Configuration Examples The following example creates a load balance profile named **apl**.

```
Ruijie(config)# load-balance-profile apl
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.13 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**] **[3rd-label] [src-ip**] [**dst-ip**] [**vlan**] [**src-port**]

no mpls field

Parameter Description

Parameter	Description
top-label	Traffic is distributed according to the top labels of the incoming MPLS packets.
2nd-label	Traffic is distributed according to the second labels of the incoming MPLS packets.
3rd-label	Traffic is distributed according to the third labels of the incoming MPLS packets.
src-ip	Traffic is distributed according to the source IP addresses of the incoming MPLS packets.
dst-ip	Traffic is distributed according to the destination IP addresses of the incoming MPLS packets.
vlan	Traffic is distributed according to the VLANs of the incoming MPLS packets.
src-port	Traffic is distributed according to the source port numbers of the incoming MPLS packets.

Defaults The default load balance mode is **src-ip** and **dst-ip**.

Command Mode Load balance enhanced profile configuration mode.

Usage Guide Use the **show load-balance-profile** command to display the load balance mode configuration.

Configuration Examples The following example sets the load balance mode of MPLS packets to **top-label** and **src-ip**.

```
Ruijie(config-load-balance-profile)# mpls field top-label src-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.14 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 Description

Parameter	Description
port-group-number	Member group ID of an aggregate port, the interface number of the aggregate port.
key-number	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 Mode Interface configuration 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 Examples The following example specifies the Ethernet interface 1/3 as a member of the static AP 3.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

3.15 show aggregateport

Use this command to display the aggregate port configuration.

show aggregateport { [*aggregate-port-number*] **summary | load-balance** }

Parameter Description

Parameter	Description
aggregate-port-number	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 Mode Any mode

Usage Guide If the aggregate port number is not specified, all the aggregate port information will be displayed.

Configuration Examples The following example displays the aggregate port configuration.

```
Ruijie# show aggregateport 1 summary
```

```
AggregatePort  MaxPorts       SwitchPort Mode    Load balance
Ports
-------------  --------------- ---------- ------
---------------------------- ------------------------
Ag1            8               Enabled     ACCESS   dst-mac
Gi0/2
```

Related Commands	Command	Description
	aggregateport load-balance	Configures a load-balance algorithm of AP.

Platform Description N/A

3.16 show lacp summary

Use this command to display the LACP aggregation information.

show lacp summary [*key*]

Parameter Description	Parameter	Description
	key	Specifies the aggregation group id to show. If it is not specified, all aggregation group information is displayed by default.

Defaults N/A

Command Mode Any mode.

Usage Guide N/A

Configuration Examples The following example displays the LACP aggregation information.

```
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                Oper    Port     Port
Port     Flags     Priority     Dev ID       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 Description N/A

3.17 show load-balance-profile

Use this command to display the enhanced profile.

show load-balance-profile [*profile-name*]

Parameter

Parameter	Description

Description		
	profile-name	Specifies the profile name.

Defaults -

Command Mode Any mode.

Usage Guide All enhanced profiles are displayed if the profile name is not specified.

Configuration Examples The following example displays configuration information in profile **module0**.

```
Ruijie# show load-balance-profile  module0
Load-balance-profile: module0
Packet   Hash Field:
IPV4: src-ip dst-ip
IPV6: src-ip dst-ip
L2  : src-mac dst-mac vlan
MPLS: top-labe l2nd-label
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.18 show aggregateport capacity

Use this command to display the AP capacity mode and the AP number.

show aggregateport capacity

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the AP capacity mode and the AP number.

```
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

3.19 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-ip**] [**dst-ip**] [**src-port**] [**dst-port**] [**src-mac**] [**dst-mac**] [**l4-src-port**] [**l4-dst-port**] [**l2-etype**] [**protocol**] [**ing-nick**] [**egr-nick**]

no mpls field

Parameter Description

Parameter	Description
vlan	Load balance based on the VLAN ID of the TRILL packet.
src-ip	Load balance based on the source IP address of the TRILL packet.
dst-ip	Load balance based on the destination IP address of the TRILL packet.
src-port	Load balance based on the source port number of the TRILL packet.
dst-port	Load balance based on the destination port number 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.
l4-src-port	Load balance based on the L4 source port number of the TRILL packet.
l4-dst-port	Load balance based on the L4 destination port number of the TRILL packet.
l2-etype	Load balance based on the Ethernet type of the TRILL packet.
protocol	Load balance based on the protocol type of the TRILL packet.
ing-nick	Load balance based on Ingress Rbridge Nickname of the TRILL packet.
egr-nick	Load balance based on Egress Rbridge Nickname of the TRILL packet.

Defaults The default load balance mode is **src-mac, dst-mac** and **vlan**.

Command Mode Load balance template configuration 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
interface-id	Layer-2 Ethernet interface or layer-2 AP port.
range *interface-range*	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 *interface-id* **switchport**	Displays the layer-2 interfaces.

Platform Description N/A

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
vlan-name	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 Examples

```
Ruijie(config)# vlan 10
Ruijie(config-vlan)# name vlan10
```

Related Commands

Command	Description
show vlan	Displays member ports of the VLAN.

Platform Description N/A

4.3 show vlan

Use this command to display member ports of the VLAN.

show vlan [**id** *vlan-id*]

Parameter Description

Parameter	Description
vlan-id	VLAN ID

Defaults N/A

Command mode All modes

Usage Guide To return to the privileged EXEC mode, input **end** or pressing **Ctrl+C**.
To return to the global configuration mode, input **exit**.

Configuration Examples

```
Ruijie# show vlan id 1
VLAN Name      Status    Ports
---------- ------------- ------------
1   VLAN0001        STATIC    Fa0/1, Fa0/2
```

Related Commands

Command	Description
name	VLAN name.
switchport access	Adds the interface to a VLAN.

Platform Description N/A

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** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter Description

Parameter	Description
vlan-id	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 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** | **hybrid** | **uplink** | **dot1q-tunnel** }

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.
hybrid	Configures the switch port as a hybrid port.
uplink	Configures the switch port as an uplink port.
dot1q-tunnel	Configures the switch port as a 802.1Q tunnel port.

Defaults By default, the switch port is an access port.

Command mode Interface configuration mode.

Usage Guide If a switch port mode is access port, it can be the member port of only one VLAN. Use the **switchport access vlan** command 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 the **switchport trunk** command to define the allowed-VLANs list.

Configuration 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	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description N/A

4.6 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.
vlist	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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.7 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
vlan-id	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 Description N/A

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.
vlan-list	Specifies the VLAN.

Defaults The trunk/unlink 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
vlan-id	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 unlink 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 N/A

Description

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
vlan-id	VLAN ID Default VLAN (VLAN 1) cannot be removed.
vlan-range	VLAN ID range.

Defaults The default is static VLAN.

Command mode Global configuration mode.

Usage Guide To return to the privileged EXEC mode, input **end** or pressing **Ctrl+C**.

To return to the global configuration mode, input **exit.**

Configuration Examples

```
Ruijie(config)# vlan 1
Ruijie(config-vlan)#
```

Related Commands

Command	Description
show vlan	Displays member ports of the VLAN.

Platform Description N/A

5 Super-VLAN Commands

5.1 subvlan

Use this command to set the sub VLAN for the super VLAN. Use the **no** form of this command to restore the default setting.

subvlan *vlan-id-list*

no subvlan [*vlan-id-list*]

Parameter Description

Parameter	Description
vlan-id-list	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 Examples The following example sets the sub VLAN for the super VLAN.

```
Ruijie(config)# vlan 3
Ruijie(config-vlan)# supervlan
Ruijie(config-vlan)# subvlan 5
Ruijie(config-vlan)# subvlan 7-19
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

5.2 subvlan-address-range

Use this command to set the IP address range of the sub VLAN. Use the **no** form of this command to restore the default setting.

subvlan-address-range *start-ip end-ip*

no subvlan-address-range

Parameter Description

Parameter	Description

start-ip	The start IP address of this sub VLAN
end-ip	The end IP address of this sub VLAN

Defaults No IP address range is set by default.

Command mode VLAN configuration Mode.

Usage Guide To return to the privileged EXEC mode, input **end** or press **Ctrl+C**.
To return to the global configuration mode, input **exit**.

Configuration Examples The following example sets the IP address range for the sub VLAN.

```
Ruijie(config)# vlan 3
Ruijie(config-vlan)# subvlan-address-range
192.168.3.10 192.168.3.100
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

5.3 supervlan

Use this command to set the VLAN as a super VLAN. Use the **no** form of this command to restore the default setting.
supervlan
no supervlan

Parameter Description

Parameter	Description
N/A	N/A

Defaults No super VLAN is set by default.

Command mode VLAN configuration Mode.

Usage Guide To return to the privileged EXEC mode, input **end** or press **Ctrl+C**.
To return to the global configuration mode, input **exit**.

Configuration Examples The following example sets the VLAN as a super VLAN.

```
Ruijie(config)# vlan 3
```

```
Ruijie(config-vlan)# supervlan
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

5.4 proxy-arp

Use this command to enable the ARP agent function for a VLAN. Use the **no** form of this command to disable this function.

proxy-arp

no proxy-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command mode VLAN configuration Mode.

Usage Guide To return to the privileged EXEC mode, input **end** or press **Ctrl+C**.
To return to the global configuration mode, input **exit**.

Configuration Examples The following example enables the ARP agent function for VLAN 3.

```
Ruijie(config)# vlan 3
Ruijie(config-vlan)# proxy-arp
```

Related Commands

Command	Description
show supervlan	Displays the super VLAN information.

Platform Description N/A

5.5 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
vlan-id	VLAN ID

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the configuration of the super VLAN and its sub VLANs.

```
Ruijie# show supervlan
supervlan id  supervlan arp-agent  subvlan id  subvlan arp-agent  subvlan ip
range
-------    ----------  -------------    -----------------
3               ON          4               ON
                            5               ON
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6 Protocol VLAN Commands

6.1 protocol-vlan ipv4 addr mask addr vlan id

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
addr	IP address in the x.x.x.x format.
id	VLAN ID, the maximal VLAN the product supports

Defaults N/A

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
```

Related Commands

Command	Description
show protocol-vlan ipv4	N/A
no protocol-vlan ipv4 *addr* **mask** *addr*	N/A
no protocol-vlan ipv4	N/A

Platform Description N/A

6.2 protocol-vlan ipv4

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 N/A

Configuration Examples The following example enables the subnet VLAN.

```
Ruijie(config-if)# protocol vlan ipv4
```

Related Commands

Command	Description
no protocol-vlan ipv4	N/A

Platform Description N/A

6.3 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
num	Profile indexes
type	Type of message and Ethernet
value	Service access point type.

Defaults N/A

Command mode Global configuration mode.

Usage Guide This function is disabled by default.

Configuration Examples The following example configures the profile for the VLAN.

```
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 *num*	N/A
no protocol-vlan profile	N/A
no protocol-vlan profile *num*	N/A

Platform Description N/A

6.4 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
num	Profile indexes
id	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 Examples The following example applies profile 1 to VLAN 101.

```
Ruijie(config-if)# protocol-vlan profile 1 vlan 101
```

Related Commands

Command	Description
show protocol-vlan profile	N/A
show protocol-vlan profile *num*	N/A

no protocol-vlan profile	N/A
no protocol-vlan profile *num*	N/A

Platform Description N/A

6.5 show protocol-vlan

Use this command to display a protocol VLAN.

show protocol-vlan [**profile** [*id*] | **ipv4**]

Parameter Description

Parameter	Description
id	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

7 Private VLAN Commands

7.1 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 Description N/A

7.2 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
svlist	The secondary VLAN list
add *svlist*	Adds the associated secondary VLAN.
remove *svlist*	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
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description N/A

7.3 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
svlist	Secondary VLAN list.
add *svlist*	Adds the associated secondary VLAN.
remove *svlist*	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

7.4 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 N/A

Configuration Examples The following example declares the private VLAN mode of the interface.

```
Ruijie(config)# interface gigabitEthernet0/2
Ruijie(config-if)# switchport mode private-vlan host
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description N/A

7.5 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
p_vid	Primary VID.
s_vid	Secondary VID

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 the host port.

```
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-asscioation
Ruijie(config-if)# switchport private-vlan host-association 22 25
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description N/A

7.6 switchport private-vlan mapping

Use this command to configure the secondary VLAN for the hybrid 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 Description

Parameter	Description
p_vid	Primary VID
svlist	Secondary VLAN list.

Defaults This function is disabled by default.

Command mode Hybrid interface configuration mode of private VLAN

Usage Guide N/A

Configuration Examples The following example configures the secondary VLAN for the hybrid port.

```
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 Description N/A

7.7 show vlan private-vlan

Use this command to display the private VLAN configuration.

show vlan private-vlan [**community** | **primary** | **isolated**]

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 Examples The following example displays the private VLAN configuration.

```
Ruijie# show vlan private-vlan
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8 MSTP Commands

8.1 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
H.H.H	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 Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the BPDU source MAC address check function on the interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# bpdu src-mac-check 00d0.f800.1e2f
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.2 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 Examples The following example enables BPDU transparent transmission.

```
Ruijie(config)# bridge-frame forwarding protocol bpdu
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.3 clear spanning-tree counters

Use this command to clear the statistics of STP transceived packets.
clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	ID of the interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears the statistics of STP transceived packets.

Examples

```
Ruijie# clear spanning-tree counters
```

Related Commands

Command	Description
show spanning-tree counters	Displays the statistics of STP transceived packets.

Platform Description N/A

8.4 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
interface-id	ID of the interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# clear spanning-tree detected-protocols
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

8.5 clear spanning-tree mst topochange record

Use this command to clear STP topology change record.

clear spanning-tree mst *instance-id* **topochange record**

Parameter

Parameter	Description

Description

instance-id	Instance ID. For STP and RSTP protocols, only instance 0 is valid.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears STP topology change record.

```
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	N/A

Platform Description N/A

8.6 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 Mode Global configuration mode

Usage Guide If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.

Configuration Examples The following example enables BPDU TUNNEL globally.

```
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 Description N/A

8.7 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 Examples The following example enables BPDU TUNNEL on the interface.

```
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

8.8 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
mac-address	The STP address for transparent transmission.

Defaults The defualt 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 Examples The following example configures the STP address for transparent transmission through BPDU TUNNEL.

```
Ruijie(config)# l2protocol-tunnel stp tunnel-dmac 011a.a900.0005
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.9 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 Examples The following example displays BPDU TUNNEL configuration.

```
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 Description N/A

8.10 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.

Usage Guide N/A

Configuration Examples The following example displays the global spanning-tree configuration.

```
Ruijie# show spanning-tree hello-time
```

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 Description N/A

8.11 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
interface-id	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.

Usage Guide N/A

Configuration Examples The following example displays the STP configuration of the interface.

```
Ruijie#  show spanning-tree interface gigabitethernet 1/5
```

Related Commands

Command	Description
spanning-tree bpdufilter	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 Description N/A

8.12 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.
instance-id	Instance number
interface-id	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 Examples The following example displays the information of MST and instances.

```
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 Description N/A

8.13 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
instance-id	Instance 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 STP topology change record of instance 0.

```
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

8.14 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 *seconds*	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 *seconds*	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 *seconds*	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 Mode Global configuration 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*(Hello Time+1.0snd) <= Max-Age Time <= 2*(Forward-Delay–1.0snd)
If the values do not according with the condition, the settings do not work.

Configuration Examples The following example enables the spanning-tree function.

```
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 Description N/A

8.15 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
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example enables Autoedge on the interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# spanning-tree autoedge disabled
```

Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration information of the interface.

Platform Description N/A

8.16 spanning-tree bpdufilter

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 bpdufilter [**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 Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example enables BPDU filter on the interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# spanning-tree bpdufilter enable
```

Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

8.17 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 N/A

Configuration Examples The following example enables the BPDU guard function on the interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# spanning-tree bpduguard enable
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

8.18 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 Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default. .

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration The following example sends the message selectively carried with MSTI according to the interface

Examples attibute of current port to realize interconnection with other vendors.

```
Ruijie(config)# spanning-tree compatible enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.19 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 can not 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 Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example enables **loop guard** on the interface.

```
Ruijie(config)# spanning-tree guard loop
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.20 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 Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example disables **guard** on the interface.

```
Ruijie(config)# spanning-tree guard none
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.21 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 N/A

Configuration The following example enables **root guard** on the interface.

Examples

```
Ruijie(config)# spanning-tree guard root
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.22 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 Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the tc filtering on the interface.

```
Ruijie(config-if)# spanning-tree ignore tc
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.23 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 Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the link type of the interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# spanning-tree link-type
point-to-point
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

8.24 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	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide N/A

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	N/A

Platform Description N/A

8.25 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
hop-count	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 Hot 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

8.26 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
stp	Spanning tree protocol(IEEE 802.1d)
rstp	Rapid spanning tree protocol(IEEE 802.1w)
mstp	Multiple spanning tree protocol(IEEE 802.1s)

Defaults The default is **mstp**.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the STP version.

```
Ruijie(config)# spanning-tree mode stp
```

Related Commands

Command	Description
show spanning-tree	Displays the spanning-tree configuration.

Platform Description N/A

8.27 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

Parameter	Description

Description

N/A	N/A

Defaults By default, all VLANs are mapped to the instance 0, *name* is empty, and *revision* is 0.

Command Mode Global configuration 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 use the following commands to configure parameters:
instance instance-id vlan vlan-range: Adds the VLANs to the MST instance. The range of instance-id is 0 to 64 and the range of VLAN is 1 to 4095. The vlan-range can be a collection of some inconsecutive VLANs separated with comma or some consecutive VLANs in the form of start VLAN number–end VLAN number. For example, instance 10 vlan 2,3,6-9 means that VLANs 2, 3, 6, 7, 8, 9 are added to instance 10. By default, all VLANs are in Instance0. To remove a VLAN from an instance, use the no form of the command: no instance instance-id [vlan vlan-range]. (In this case, the range of instance is 1 to 64).
name name: Specify the MST name, a string of up to 32 characters. You can use the no name command to restore it to the default setting.
revision version: Set the MST versions in the range 0 to 65535. You can use the no name command to restore it the default setting.
show spanning-tree mst configuration: Shows the information of the MST region.

Configuration Examples This example enters the MST configuration mode, and maps VLANs 3. 5 to 10 to MST instance 1:

```
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
MST configuration
Name [region1]
Revision 1
Instance  Vlans Mapped
----------  --------------------
0       1-2,4,11-4094
1       3,5-10
-----------------------------------
Ruijie(config-mst)# exit
Ruijie(config)#
```

The following example removes VLAN 3 from instance 1.

```
Ruijie(config-mst)# no instance 1 vlan 3
```

The following example deletes instance 1.

```
Ruijie(config-mst)# no instance 1
```

You can verify your settings by entering the **show** command of the MST configuration commands.

Related Commands

Command	Description
show spanning-tree mst	Displays the MST region configuration.
instance *instance-id* **vlan** *vlan-range*	Adds VLANs to the MST instance.
name	Configures the name of MST.
revision	Configures the version of MST.

Platform Description N/A

8.28 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 Mode Interface configuration mode.

Usage Guide A higher cost value means a higher path cost.

Configuration Examples This example sets the path cost to 400 on the interface associated with instances 3.

```
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

Command	Description

Commands

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 Description N/A

8.29 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
Instance-id	Instance ID, in the range of 0 to 64
priority	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.

Configuration Examples This example sets the priority of **gigabitethernet 1/1** to 10 in instance 20.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# 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 Description N/A

8.30 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
instance-id	Instance ID, in the range of 0 to 64
priority	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 N/A

Configuration Examples The following example sets the device priority of the Instance to 8192.

```
Ruijie(config-if)# 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 Description N/A

8.31 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 Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the path cost of the port.

```
Ruijie(config-if)# spanning-tree pathcost method long
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

8.32 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	Disables the portfast on the interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example enables the portfast on the interface.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# spanning-tree portfast
```

Related Commands

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

8.33 spanning-tree portfast bpdufilter 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 bpdufilter default

no spanning-tree portfast bpdufilter default

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default,

Command Mode Global configuration 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 Examples The following example enables the BPDU filter function globally.

```
Ruijie(config)# spanning-tree portfast bpdufilter default
```

Related Commands

Command	Description
show spanning-tree interface	Displays the global STP configuration.

Platform Description N/A

8.34 spanning-tree portfast bpduguard default

Use this command to enable the GPDU 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 Mode Global configuration 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.

Configuration Examples The following example enables the GPDU guard globally.

```
Ruijie(config)# spanning-tree portfast bpduguard
default
```

Related Commands

Command	Description
show spanning-tree interface	Displays the global STP configuration.

Platform Description N/A

8.35 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

8.36 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 N/A

Configuration Examples The following example restores the **spanning-tree** configuration to the default setting.

```
Ruijie(config)# spanning-tree reset
```

Related Commands

Command	Description
show spanning-tree	Displays the global STP configuration.
show spanning-tree interface	Displays the STP configuration of the interface.

Platform Description N/A

8.37 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 Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables **tc-guard** on the interface to prevent the spread of TC messages.

```
Ruijie(config)# spanning-tree tc-guard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.38 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

8.39 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 N/A

Configuration Examples The following example enables tc-guard to prevent TC packets from being flooded.

```
Ruijie(config)# spanning-tree tc-protection tc-guard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.40 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
tx-hold-count	Maximum number of the BPDU messages sent in one second, 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 maximum number of the BPDU messages sent in one second.

```
Ruijie(config)# spanning-tree tx-hold-count 5
```

Related Commands

Command	Description
show spanning-tree	Displays the global MSTP configuration.

Platform Description N/A

9 GVRP Commands

9.1 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 Examples The following example enables GVRP PDUs transparent transmission.

```
Ruijie(config)# bridge-frame forwarding protocol gvrp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.2 clear gvrp statistics

Use this command to clear the GVRP statistics for re-counting.

clear gvrp statistics { *interface-id* | **all** }

Parameter Description

Parameter	Description
interface-id	Interface id

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide Use the **show gvrp statistics** to display the statistics.

Configuration Examples The following example clears GVRP statistics.

```
Ruijie# clear gvrp statistics all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.3 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 Examples The following example configures the GVRP advertisement mode on the interface.

```
Ruijie(config-if)# gvrp applicant state normal
```

Related Commands

Command	Description
show gvrp configuration	Displays the GVRP configurations.

Platform Description N/A

9.4 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 Examples The following example enables dynamic VLAN creation.

```
Ruijie(config)# gvrp dynamic-vlan-creation enable
```

Related Commands

Command	Description
show gvrp configuration	Displays the GVRP configurations.

Platform Description N/A

9.5 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 Examples The following example enables the GVRP function.

```
Ruijie(config)#gvrp enable
```

Related Commands

Command	Description
show gvrp configuration	Displays the GVRP configurations.

Platform Description N/A

9.6 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
N/A	N/A

Defaults Dynamic VLAN creation/registration/canceling is enabled by default,

Command mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the registration mode.

```
Ruijie(config-if)# gvrp registration mode normal
```

Related Commands

Command	Description
show gvrp configuration	Displays the GVRP configurations.

Platform N/A

Description

9.7 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
join *timer_value*	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.
leave *timer_value*	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.
leave all *timer_value*	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 leaveall to leaveall+join.

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 Examples The following example configures the join timer.

```
Ruijie(config)# gvrp timer join 200
```

Related Commands

Command	Description
show gvrp configuration	Displays the GVRP configuration.

Platform Description N/A

9.8 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 Examples The following example enables GVRP PDUs TUNNEL globally.

```
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 Description N/A

9.9 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 Examples The following example enables GVRP PDUs TUNNEL on the interface.

```
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

9.10 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
mac-address	The MAC address for transparent transmission in GVRP PDUs TUNNEL.

Defaults The default is 01d0.f800.0006.

Command mode Global configuration mode

Usage Guide The available MAC address f ranges from 01d0.f800.0006 to 011a.a900.0006.

Configuration Examples The following example configures the MAC address for transparent transmission in GVRP PDUs TUNNEL.

```
Ruijie(config)# l2protocol-tunnel gvrp tunnel-dmac 011a.a900.0006
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.11 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 Examples The following example displays GVRP configuration.

```
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 Description N/A

9.12 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
interface-id	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 Examples

```
Ruijie# show gvrp statistics gigabitethernet 1/1
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 unvalid 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 Description N/A

9.13 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 Examples The following example displays the GVRP status.

```
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 Description N/A

9.14 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 Examples The following example displays GVRP PDUs TUNNEL configuration.

```
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

10 LLDP Commands

10.1 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 Description

Parameter	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
ca-word	Address information

Defaults N/A

Command Mode LLDP Civic address configuration mode

Usage Guide This command is used to configure a common LLDP address in LLDP Civic address configuration mode.

Configuration Examples The following example configures an LLDP Civic Address (ID: 1).

```
Ruijie#config
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
```

Related Commands

Command	Description
show lldp location civic-location { **identifier** *id* **| interface** *interface-name* **| static** }	Displays the information about an LLDP Civic address.

Platform Description N/A

10.2 clear lldp statistics

Use this command to clear LLDP statistics.

clear lldp statistics [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide **interface** parameter: clear the LLDP statistics of the specified interface

Configuration Examples The following example clears LLDP statistics of interface 1.

```
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 Description N/A

10.3 clear lldp table

Use this command to clear LLDP neighbor information.

clear lldp table [**interface** *interface-name*]

Parameter Description	Parameter	Description
	interface-name	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 Examples The following example clears the LLDP neighbor information on interface 1.

```
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 Description N/A

10.4 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 Description	Parameter	Description
	device-type	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** *id* **| interface** *interface-name* **| static** }	Displays LLDP Civic Address information.

Platform Description N/A

10.5 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 Description	Parameter	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 Examples The following example disables LLDP globally and on the interface.

```
Ruijie#config
Ruijie(config)#no lldp enable
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)# no lldp enable
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform Description N/A

10.6 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 Description	Parameter	Description
	N/A	N/A

Defaults By default, Ethernet II encapsulation format is used.

Command Mode Interface configuration mode.

Usage Guide

⚠ To guarantee the normal communication between local device and neighbor device, the same

LLDP packet encapsulation format must be used.

Configuration Examples

```
The following example sets LLDP packet encapsulation format to
SNAP.Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp encapsulation snap
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

10.7 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 Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration 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 Examples The following example configures LLDP error detection.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp error-detect
```

Related Commands

Command	Description
show interface status	Displays LLDP status information.

Platform N/A

Description

10.8 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 Description

Parameter	Description
value	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.

```
Ruijie#config
Ruijie(config)#lldp fast-count 5
```

Related Commands

Command	Description
show interface status	Displays LLDP status information.

Platform Description N/A

10.9 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 Description

Parameter	Description
value	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.

```
Ruijie#config
Ruijie(config)#lldp hold-multiplier 5
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

10.10 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 Description

Parameter	Description
id	ID of a common address of a network device, in the range from 1 to 1024.

Defaults N/A

Command Mode Global configuration 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 Commands

Command	Description
show lldp location civic-location { **identifier**	Displays the LLDP Civic Address information.

id **| interface** *interface-name* **| static** }	

Platform Description N/A

10.11 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 Description

Parameter	Description
id	ID of an emergency number, in the range from 1 to 1024.
tel-number	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 Examples The following example sets an emergency number.

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
```

Related Commands

Command	Description
show lldp location elin-location { **identifier** *id* **| interface** *interface-name* **| static }**	Displays an LLDP emergency number.

Platform Description N/A

10.12 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 Description

Parameter	Description
ip-address	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 Description N/A

10.13 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 Description N/A

10.14 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 Description

Parameter	Description
profile-num	ID of an LLDP network policy, in the range from 1 to 1024.

Defaults N/A

Command Mode Global configuration 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.

```
Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)#
```

Related Commands

Command	Description
show lldp network-policy profile [*profile-num*]	Displays an LLDP network policy.

Platform Description N/A

10.15 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 Description

Parameter	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

10.16 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		
	seconds	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 Examples The following example sets the interval of sending LLDP Traps to 10 seconds.

```
Ruijie#config
Ruijie(config)#lldp timer notification-interval 10
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform Description N/A

10.17 lldp timer reinit-delay

Use this command to set port initialization delay. Use the **no** form of this command to restore he default setting.

lldp timer reinit-delay *seconds*

no lldp timer reinit-delay

Parameter Description	Parameter	Description
	seconds	Port initialization delay, in the range from 1 to 10 in the unit of seconds.

Defaults The default is 2.

Command Mode Global configuration 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 Examples The following example sets LLDP port initialization delay to 3 seconds.

```
Ruijie#config
Ruijie(config)#lldp timer reinit-delay 3
```

Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform Description N/A

10.18 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 Description	Parameter	Description
	seconds	LLDP packet transmission delay, in the range from 1 to 8192 in the unit of seconds.

Defaults The default is 2.

Command Mode Global configuration 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 Description N/A

10.19 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 Description

Parameter	Description
seconds	Interval of sending the LLDP packets, in the range from 5 to 32768 in the unit of seconds.

Defaults The default is 30.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the interval of sending the LLDP packets to 10 seconds.

```
Ruijie#config
Ruijie(config)#lldp timer tx-interval 10
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

10.20 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
	vlan-id	VLAN ID
	vlan-name	VLAN Name TLV
	vlan-id	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
	id	Policy ID
	network-policy	Network Policy TLV
	profile-num	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 Mode Interface configuration 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 Examples

The following example configures all IEEE 802.1 TLVs to be advertised.

```
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 Description

N/A

10.21 { 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 Description

Parameter	Description
voice	Voice application
voice-signaling	Voice-signaling application

vlan-id	(Optional) VLAN ID of voice flow. The value ranges from 1 to 4094.
cos	(Optional) Class of service
cvalue	(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
dvalue	(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 Mode LLDP network policy configuration 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 Commands

Command	Description
show lldp network-policy profile [*profile-num*]	Displays the LLDP network policy.

Platform Description N/A

10.22 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 Description

Parameter	Description
interface-name	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 Examples The following example displays the device information to be sent to neighbor device.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

10.23 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 Description

Parameter	Description
civic-location	Encapsulates a common address of a network device.
elin	Encapsulates an emergency number.
identifier	Displays one address or emergency number configured.
id	Policy ID of configured information
interface	Displays the address or emergency number on an interface.
interface-name	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 static
Elin location information
--------------------------
Identifier : t
Elin  : iiiiiiiiii
Ports     : Gi1/0/3
--------------------------
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.24 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
	interface-name	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: ● 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 Description N/A

10.25 show lldp network-policy profile

Use this command to display the information about an LLDP network policy.

show lldp network-policy profile [*profile-num*]

Parameter Description

Parameter	Description
profile-num	ID of a network policy, in the range from 1 to 1024.

Defaults N/A

Command Mode Privileged EXEC 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 Profile 1
 voice vlan 2 cos 4 dscp 6
 voice-signaling vlan 2000 cos 4 dscp 6
 Interface:
 GigabitEthernet1/0/16
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.26 show lldp statistics

Use this command to display LLDP statistics.

show lldp statistics [**global** | **interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	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 Description N/A

10.27 show lldp status

Use this command to display LLDP status information.

show lldp status [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	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 Commands

Command	Description
N/A	N/A

Platform Description N/A

10.28 show lldp tlv-config

Use this command to display the advertisable TLV configuration of a port.

show lldp tlv-config [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	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

11 QinQ Commands

11.1 dot1q new-outer-vlan 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 *vid* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*

no dot1q new-outer-vlan *vid* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*

Parameter Description

Parameter	Description
v_list	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

11.2 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** 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
v_list	Inner vlan id list
vid	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 setss 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** *intf-id*]	N/A

Platform Description N/A

11.3 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** 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*

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 Mode Interface configuration 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** *intf-id*]	N/A

Platform Description N/A

11.4 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** 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*

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 Mode Interface configuration 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** *intf-id*]	N/A

Platform Description N/A

11.5 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

Parameter Description

Parameter	Description
no	Cancels the priority mapping of the packets on the interface.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A

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 Description N/A

11.6 frame-tag tpid

Use this command to set the packet TPID compatible with the manufacturer TPID. Use the **no** form of this command to restore the default setting.

frame-tag tpid *tpid*

no 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 N/A

Configuration Examples The following example sets the packet TPID compatible with the manufacturer TPID.

```
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 Description N/A

11.7 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** form of this command to restore the default setting.

inner-priority-trust enable

no inner-priority-trust enable

Parameter Description

Parameter	Description
no	Removes the settings.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example copies the priority of the inner tag to the outer tag of the packets on the interface.

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# inner-priority-trust enable
```

Related Commands

Command	Description
show inner-priority-trust	N/A

Platform Description N/A

11.8 l2protocol-tunnel

Use this command to set the dot1q-tunnel port to receive L2 protocol message. Use the **no** form of this command to disable this function.

l2protocol-tunnel { **stp | gvrp** }

no 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 N/A

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 Description N/A

11.9 l2protocol-tunnel enable

Use this command to enable transparent transmission of L2 protocol message. Use the **no** 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 N/A

Command Mode Intereface configuration mode.

Usage Guide N/A

Configuration Examples Here is an example of enabling transparent transmission of L2 protocol message :

```
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 Description N/A

11.10 l2protocol-tunnel tunnel-dmac

Use this command to set the MAC address for the transparent transmission of the corresponding protocol messages. Use the no 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*

Parameter Description

Parameter	Description
stp	Sets the STP transparent transmission address.
gvrp	Sets the GVRP transparent transmission address.
mac-address	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 Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the MAC address for the L2-protocol transparent transmission function:

```
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 Description N/A

11.11 mac-address-mapping index-id 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** form of this command to restore the default setting.
mac-address-mapping *index-id* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*
no mac-address-mapping *index-id* **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 Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example copies the MAC addresses dynamically-learned from the source VLANs 1-3 to the destination VLAN 5.

```
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 Description N/A

11.12 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 Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays whether dot1q-tunnel of interface is enabled or not.

```
Ruijie# show dot1q-tunnel
Ports   Dot1q-tunnel
-----   ---------
Gi0/1    Enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

11.13 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 Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the configuration of interface tpid.

```
Ruijie# show frame-tag tpid
Ports    tpid
-----  ---------
Gi0/1    0x9100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.14 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 Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays whether the priority copy function is enabled.

```
Ruijie# show inner-priority-trust
Port    inner-priority-trust
----    ----------
Gi0/1    enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

11.15 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 Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the VLAN configuration on the dot1q-tunnel port.

```
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

11.16 show interfaces remark

Use this command to display the priority mapping configuration.

show interfaces[*intf-id*] **remark**

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 priority mapping configuration.

```
Ruijie# show interfaces remark
Ports        Type        From value  To value
------------ ----------- ----------- --------
Gi0/1        Cos-To-Cos  3           5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.17 show interfaces mac-address-mapping

Use this command to display the MAC address mapping configuration.

show interfaces mac-address-mapping *index-id*

Parameter Description

Parameter	Description
index-id	Policy ID of copying MAC addresses.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the MAC address mapping configuration.

```
ruijie# show interfaces mac-address-mapping 1
Ports         Destination-VID  Source-VID-list
------------ ---------------- ---------------
Gi0/1         5                1-3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

11.18 show l2protocol-tunnel

Use this command to display transparent transmission configuration of L2 protocol.

show l2protocol-tunnel { **gvrp** | **stp** }

Parameter

Parameter	Description

Description

gvrp	Displays configuration of transparently transmitting gvrp protocol.
stp	Displays configuration of transparently transmitting stp protocol.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays transparent transmission configuration of L2 protocol.

```
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 Description N/A

11.19 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 Null policy list.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays vid add policy list of prorocol-based dot1q-tunnel port.

```
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

11.20 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 Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays flow-based vid change or add policy list.

```
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 Description N/A

11.21 show translation-table

Use this command to display vid modify policy list of prorocol-based access, trunk, hybrid port.

show translation-table [**interface** *intf-id*]

Parameter Description

Parameter	Description
intf-id	Specifies the interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays vid modify policy list of prorocol-based access, trunk, hybrid port.

```
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 Description N/A

11.22 switchport dot1q-tunnel allowed vlan

Use this command to configure the allowed VLAN of dot1q-tunnel. Use the no form of this command to restore the default setting.

switchport dot1q-tunnel allowed vlan [**add**] { **tagged|untagged** } *v_list*

switchport dot1q-tunnel allowed vlan remove *v_list*

no switchport dot1q-tunnel allowed vlan

Parameter Description

Parameter	Description
add	Add allowed VLAN.
tagged	Tag-carried.

untagged	Not tag-carried.
v_list	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 Description N/A

11.23 switchport dot1q-tunnel native vlan

Use this command to configure the default vlan id of dot1q-tunnel. Use the no form of this command to restore the default setting.

switchport dot1q-tunnel native vlan *vid*

no switchport dot1q-tunnel native vlan

Parameter Description

Parameter	Description
vid	Configures default vlan id.
no	Configures default vlan as 1.

Defaults The default is VLAN 1.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies default VLAN of dot1q-tunnel port as 8.

```
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 Description N/A

11.24 switchport mode dot1q-tunnel

Use this command to configure the interface as the dot1q-tunnel interface. Use the **no** form of this command to restore the default setting.

switchport mode dot1q-tunnel

no switchport mode

Parameter Description

Parameter	Description
no	Deletes the corresponding dot1q-tunnel interface configuration.

Defaults The interface is not a tunnel port by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the interface as the dot1q-tunnel interface.

```
Ruijie(config)# interface gi 0/1
Ruijie(config-if)# switchport access vlan 22
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config)# end
```

Related Commands

Command	Description
show vlan	N/A

Platform Description N/A

11.25 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** 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**

Parameter Description

Parameter	Description
acl	Flow matching.
vid	Modified inner vid
no	Removes the settings.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies the outer vid of outgoing messages whose source address is 1.1.1.2 as 6,

```
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 Description N/A

11.26 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** 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**

Parameter Description

Parameter	Description
acl	Flow matching.
vid	vid list to be added.
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 the vid of input message whose source address is 1.1.1.3 as 9.

```
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 Description N/A

11.27 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** 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**

Parameter Description

Parameter	Description
acl	Flow matching.

vid	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

12 Management Ethernet Interface Commands

12.1 clear arp-cache oob

Use this command to delete dynamic ARP mapping records from the ARP cache table on the MGMT interface.

clear arp-cache oob [*ip* [*mask*]]

Parameter Description

Parameter	Description
ip	IP address. The ARP entry with the specified IP address is deleted. If the keyword "trusted" is specified, the trusted ARP entries are deleted. Otherwise, dynamic ARP entries are deleted.
mask	Subnet mask, that is, subnet in which ARP entries will be deleted. The IP address must be a subnet number. If the keyword "trusted" is specified, the trusted ARP entries of the subnet are deleted. Otherwise, the dynamic ARP entries of the subnet are deleted.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to update the ARP cache table.

Configuration Examples The following example deletes all dynamic ARP mapping records from the cache table.

```
clear arp-cache oob
```

The following example deletes dynamic ARP entry 1.1.1.1.

```
clear arp-cache oob 1.1.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.2 clear ipv6 neighbors oob

Use this command to clear the neighbor learned dynamically.

clear ipv6 neighbors oob

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the neighbor learned dynamically on the MGMT interface.

Configuration Examples The following example clears the dynamic ARP entries on the MGMT interface.

```
Ruijie# clear ipv6 neighbors oob
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.3 copy

Use this command to copy the files between the local host and the network host.

copy *source-url destination-url*

Parameter Description

Parameter	Description
source-url	Source URL to copy the destination file.
destination-url	Destination URL to copy the destination file.

Defaults N/A

Command mode Privileged EXECmode

Usage Guide The **tftp** can be specified as the prefix of the command **copy** url. Modify the prefix to **oob_tftp** for the management of the copy of files in the network node.

Configuration Examples The following example downloads RG0S.bin from TFTP server 192.168.1.1 on the management network.

```
Ruijie#copy oob_tftp://192.168.1.1/rgos.bin flash:rgos.bin
```

The following example downloads RG0S.bin from TFTP server 2001:1::1 on the management network.

```
Ruijie# copy oob_tftp://2001:1::1/RGOS.bin flash:RGOS.bin
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.4 gateway

Use this command to configure the default gateway address for the MGMT interface.

gateway *address*

Parameter Description

Parameter	Description
address	The default gateway address for the IPv4 communication on the MGMT interface.

Defaults No gateway is configured by default,

Command mode Interface configuration mode

Usage Guide The interface type is MGMT and the interface number is constantly 0.

Configuration Examples The following example configures the default gateway for the MGMT interface:

```
Ruijie#config
Ruijie(config)#interface mgmt 0
Ruijie(config-if-Mgmt 0)#gateway 192.168.0.1
Ruijie(config-if-Mgmt 0)#end
```

Related Commands

Command	Description
show interface mgmt	Displays the MGMT interface configurations.

Platform Description N/A

12.5 ipv6 gateway

Use this command to configure the default gateway address for the MGMT interface.

ipv6 gateway *address*

Parameter Description

Parameter	Description
ipv6-address	The default gateway address for the IPv6 communication on the MGMT interface.

Defaults No gateway is configured by default,

Command mode Interface configuration mode

Usage Guide The interface type is MGMT and the interface number is constantly 0.

Configuration Examples The following example configures the default gateway for the MGMT interface:

```
Ruijie#config
Ruijie(config)#interface mgmt 0
Ruijie(config-if-Mgmt 0)# ipv6 gateway 2001:1::1
```

Related Commands

Command	Description
show interface mgmt	Displays the MGMT interface configurations.

Platform Description N/A

12.6 logging server oob

Use this command to specify the MGMT interface to send a log message to the Syslog server.

logging server oob *ip-address*

Parameter Description

Parameter	Description
ip-address	Sets the IP address for the destination host.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is only used to specify the MGMT interface to send a log message to the Syslog server.

Configuration Examples The following example sets the Syslog server IP address to 1.1.1.1.

```
Ruijie(config)# logging server oob 1.1.1.1
```

Related Commands

Command	Description
logging on	Enables the log function.
show logging	Displays log packets in the cache area and related log configuration parameters.
logging trap	Sets the level of log information that can be sent to the Syslog server.

Platform Description N/A

12.7 logging server oob ipv6

Use this command to specify the MGMT interface to send a log message to the Syslog server.

logging server oob [**ipv6**] *ipv6-address*

Parameter Description

Parameter	Description
Ipv6-address	Sets the IPv6 address for the destination host.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is only used to specify the MGMT interface to send a log to the Syslog server.

Configuration Examples The following example sets the Syslog server IPv6 address to 1000::1.

```
Ruijie(config)# logging server oob ipv6 1000::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.8 ping oob

Use this command to detect the host connectivity on the management network.

ping oob [**ip**] *ip-address*

Parameter Description	Parameter	Description
	ip-address	Sets the IP address for the destination host.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide This command is only used to detect the connectivity between the hosts on the management network..

Configuration Examples The following example detects the connectivity between host 192.168.0.1 and the MGMT interface.

```
Ruijie#ping oob 192.168.0.1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.9 ping oob ipv6

Use this command to detect the IPv6 connectivity between hosts on the management network.

ping oob [**ipv6**] *ipv6-address*

Parameter Description	Parameter	Description
	Ipv6-address	Sets the IPv6 address for the destination host.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide This command is only used to detect the IPv6 connectivity between the hosts on the management network.

Configuration Examples The following example detects the connectivity between host 2001:1::1 and the MGMT interface.

```
Ruijie# ping oob ipv6 2001:1::1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.10 telnet oob

Use this command to remotely log in to the host on the management network connected to the MGMT interface.

telnet oob *host*

Parameter Description

Parameter	Description
host	IP address or domain name of a host.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to remotely log in to the host on the management network connected to the MGMT interface.

Configuration Examples The following example logs in to host 192.168.200.1 on the management network.

```
Ruijie#telnet oob 192.168.200.1
```

The following example logs in to the IPv6 host 2001:1::1 on the management network.

```
Ruijie# telnet oob 2001:1::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.11 traceroute oob

Use this command to trace the route from the MGMT interface to the connected host on the management network.

traceroute oob [**ip**] *ip-address*

Parameter Description

Parameter	Description
ip-address	Sets the IP address for the destination host.

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide This command is used to trace the route from the MGMT interface to the connected host on the management network.

Configuration Examples The following example traces the route to host 192.168.0.1 on the management port.

```
Ruijie# traceroute oob 192.168.0.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.12 traceroute oob ipv6

Use this command to trace the route to a specified IPv6 host on the management network.

traceroute oob [**ipv6**] *ipv6-address*

Parameter Description

Parameter	Description
ipv6-address	Sets the IPv6 address for the destination host.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is only used to detect the IPv6 connectivity between the hosts on the management network.

Configuration Examples The following example traces the route to a specified IPv6 host on the management network.

```
Ruijie# traceroute ipv6 oob 2001:1::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.13 snmp-server host oob

Use this command to specify the MGMT interface to send a trap message to the NMS server.

snmp-server host oob *ip-address*

Parameter Description

Parameter	Description
ip-address	Sets the IPv4 address for the destination host.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to specify the MGMT interface to send a trap message to the NMS server.

Configuration Examples The following example sets the SNMP server IP address to 1.1.1.1.

```
Ruijie(config)# snmp-server host oob 1.1.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.14 snmp-server host oob ipv6

Use this command to specify the MGMT interface to send a trap message to the NMS server.

snmp-server host oob [**ipv6**] *ipv6-address*

Parameter Description

Parameter	Description
Ipv6-address	Sets the IPv6 address for the destination host.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to specify the MGMT interface to send a trap message to the NMS server.

Configuration Examples The following example sets the SNMP server IP address to 1000::1.

```
Ruijie(config)# snmp-server host oob ipv6 1000::1
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

12.15 show arp oob

Use this command to display the ARP cache table applied on the MGMT interface.

show arp oob [*ip* [*mask*] | **complete** | **incomplete** | *mac-address*]

Parameter Description

Parameter	Description
ip	Displays ARP entries of the specified IP address. If keyword **trusted** is specified, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed,
mask	Displays ARP entries within the IP subnet. If keyword **trusted** is specified, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed,
complete	Displays analyzed dynamic ARP entries.
incomplete	Displays unanalyzed dynamic ARP entries.
mac-address	Displays ARP entries of the specified MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the outcome of running the **show arp** 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
```

Field	Description
Protocol	The network address protocol. The field is “Internet”.
Address	The IP address corresponding to the hardware address.
Age (min)	The time period when ARP cache is preserved, measured in minutes. If this parameter is local or configured statically, it is displayed as “-”.
Hardware	The hardware address corresponding to the IP address.
Type	Both Hardware type and Ethernet address are ARPA.
Interface	The interface associated with the IP address.

The following example displays the outcome of running the **show arp oob** *192.168.195.68*.

```
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** *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   Mgmt 0
```

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

12.16 show ipv6 neighbors oob

Use this command to display the IPv6 neighbor table applied on the MGMT interface.

show ipv6 neighbors oob [**verbose**] [*ipv6-address*]

Parameter	**Parameter**	**Description**

Description	**verbose**	Displays the detailed information about the neighbor.
	ipv6-addres	Displays the information about the specified neighbor.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays information about IPv6 neighbors on the MGMT interface.

```
Ruijie# show ipv6 neighbors oob
IPv6 Address Linklayer Addr   Interface
fa::1         00d0.0000.0002   Mgmt 0
fe80::200:ff:fe00:2  00d0.0000.0002  Mgmt 0
```

The following example displays detailed information about IPv6 neighbors.

```
Ruijie# show ipv6 neighbors oob verbose
IPv6 Address  Linklayer Addr Interface
2001::1      00d0.f800.0001 Mgmt 0
       State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1    00d0.f800.0001 Mgmt 0
       State: Reach/H Age: - asked: 0
```

Field	Description
IPv6 Address	Neighbor IPv6 address,
Linklayer Addr	Link address (MAC address). If the address is not obtained, it is displayed as “incomplete”.
Interface	Neighbor interface.
State	Neighbor state: state/H(R) There are following values: INCMP(Incomplete)—During neighbor address resolution, the neighbor solicitation (NS) packets are sent but the device has not received response packets (neighbor advertisement packets) from the neighbor. REACH(Reachable)—indicates that the neighbor is reachable and the packets can be sent to the neighbor directly. STALE—indicates that the neighbor reachability is due and packets can be sent to the neighbor directly. Neighbor Unreachability Detection (NUD) will start. DELAY—indicates that packets are being sent to the neighbor in STALE state, and the state turns from STALE to DELAY. If the device does not receive NA packets from the neighbor in the period of DELAY_FIRST_PROBE_TIME (five seconds), the state turns from DELAY to PROBE and the device sends NS packets to the neighbor. NUD is ready to start. PROBE—indicates that NUD has been started to detect whether the neighbor is reachable. NS packets are sent to the neighbor every period (RetransTimer milliseconds) until the device receives the response packets or the number of NS packets reaches the MAX UNICAST SOLICIT, that is, 3. ?—indicates unknown status. /R—indicates that the neighbor is a device. /H—indicates that the neighbor is a host.
Age	Indicates the period during which the neighbor is considered reachable. “-” represents constant reachability while the static neighbor entries are an exception. Pay attention to whether they are reachable in reality. “expired” indicates that neighbor reachability is due and NUD will start.
Asked	Indicates the number of NS packets sent to the neighbor before the device resolves the link address of the neighbor.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

12.17 show mgmt virtual

Use this command to display the virtual MGMT interface information.

show mgmt virtual

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 MGMT interface information in the VSU.

```
Ruijie# show mgmt virtual
MGMT 1/0
Virtual MGMT Member:
    1/M1/MGMT0: Active
    1/M2/MGMT0: Backup
Virtual MGMT Event:
    Last GRTD Fail: N/A
    Last Link Fail: N/A
    Last Board Fail: N/A
    Last IP-Link Fail: N/A

MGMT 2/0
Virtual MGMT Member:
    1/M1/MGMT0: Active
    1/M2/MGMT0: Backup
Virtual MGMT Event:
    Last GRTD Fail: N/A
    Last Link Fail: N/A
    Last Board Fail: N/A
    Last IP-Link Fail: N/A
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

13 ERPS Commands

13.1 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
vlan-list	Sub-rings' R-APS VLAN.

Defaults By default, Ethernet ring is not associated with its sub-rings.

Command Mode ERPS configuration 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 Examples

The following example associates the Ethernet sub-ring with other Ethernet rings:

#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 Description N/A

13.2 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 Examples The following example enables the ERPS protocol globally:

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 Description N/A

13.3 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 Description N/A

13.4 erps raps-vlan *vlan-id*

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
vlan-id	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 Examples # Enter the privileged EXEC mode.

```
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

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

13.5 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
	instance-id-list	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 Mode EPRS configuration 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 Description N/A

13.6 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
interface-name1	Name of the West port.
interface-name2	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 Examples The following example is for the 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
```

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 *vlan-id*	Establish the association between the subring and other Ethernet rings in the subring ERPS configuration mode.

Platform Description N/A

13.7 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 { *interface-name1* | **virtual-channel** } **east** { *interface-name2* | **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 Description N/A

13.8 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 Examples The following example shows the use of this command.

```
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 Description N/A

13.9 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 Description N/A

13.10 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

13.11 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 Mode EPRS configuration mode.

Usage Guide

- **Holdoff timer:** This timer is used to avoid the ERPS from topology swithcingswitching 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 Examples The following example configures the timer of the ERPS protocol.

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	N/A

Platform N/A

Description

IP Address & Application 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 settings.

gateway *address*

no gateway

Parameter Description

Parameter	Description
address	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**]

no ip address [*ip-address network-mask* [**secondary**]]

Parameter Description

Parameter	Description
ip-address	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.

network-mask	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.
secondary	Indicates the secondary IP address that has been configured.

Defaults No IP address is configured for the interface by default.

Command Mode N/A

Usage Guide Interface configuration mode.

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 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.

In general, the layer-2 switch is configured with a default gateway by the **ip default-gateway** 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
```

Related Commands	Command	Description
	show interface	Displays detailed information of the interface.

Platform Description N/A

1.3 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 Description	Parameter	Description
	ip-address	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 he destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```
Ruijie(config-if)# ip broadcast-address 0.0.0.0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.4 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 Description

Parameter	Description
milliseconds	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.
bucket-size	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

1.5 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 Description

Parameter	Description
access-list-number	(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 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 Commands

Command	Description
N/A	N/A

Platform Description N/A

1.7 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 is restore the default setting.

ip mtu *bytes*

no ip mtu

Parameter Description

Parameter	Description
bytes	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 iexample 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 Commands

Command	Description
mtu	Sets the MTU value of an interface.

Platform Description N/A

1.8 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 Description

Parameter	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

1.9 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 Description	Parameter	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 Examples The following example disables the IP source route.

```
Ruijie(config)# no ip source-route
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.10 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
	value	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 Examples The following example sets the TTL value of the unicast packet to 100.

```
Ruijie(config)# ip ttl 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.11 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 Description	Parameter	Description
	interface-type	Type of the associated interface
	interface-number	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 to the following example configures the local interface as an unnumbered interface and sets the associated interfacet to FastEthernet 0/1 (an IP address is configured for the interface).

```
Ruijie(config-if)# ip unnumbered fastEthernet 0/1
```

Related Commands

Command	Description
show interface	Displays the detailed information about the interface.

Platform Description N/A

1.12 ip unreachables

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 unreachables

no ip unreachables

Parameter Description

Parameter	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 unreachables
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.13 show ip interface

Use this command to display the IP status information of an interface.

show ip interface [*interface-type interface-number* | **brief**]

Parameter Description	Parameter	Description
	interface-type	Specifies interface type.
	interface-number	Specifies interface number.
	brief	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 exmaple displays the output of the **show ip interface brirf 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 unreachabled 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 unreachabled 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 fash 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: Request packet: Reply packet: Unknown packet:	Show the total number of ARP packets received on the interface, including: ARP request 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 Description N/A.

1.14 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
interface-name	Interface name
total	Displays the total statistics of all interfaces.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays the output of this command.

```
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 This command is supported on switches.

1.15 show ip raw-socket

Use this command to display IPv4 raw sockets.

show ip raw-socket [*num*]

Parameter Description

Parameter	Description
num	Protocol.

Defaults N/A.

Command Mode Priviledged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays all IPv4 raw sockets.

```
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

1.16 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 Examples The following displays all IPv4 sockets.

```
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 Description N/A

1.17 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 Description

Parameter	Description
local-port num	Local port number

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example displays all IPv4 UDP sockets.

```
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 Description N/A

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 commandto restore the default setting.

arp *ip-address MAC-address type* [**alias**]

no arp *ip-address MAC-address type* [**alias**]

Parameter Description

Parameter	Description
ip-address	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
MAC-address	48-bit data link layer address
type	ARP encapsulation type. The keyword is arpa for the Ethernet interface.
alias	(Optional) RGOS will respond to the ARP request from this IP address after this parameter is defined.

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

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. 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 Description

Parameter	Description
num	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 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 Description

Parameter	Description
limit	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*

no arp gratuitous-send

Parameter Description

Parameter	Description
seconds	The time interval to send the free ARP request message in the range from 1 to 3600 in the unit of seconds.

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 Description N/A

2.5 arp oob

Use this command to configure the static ARP on the management port. Use the **no** form of this command to restore the default setting.

arp oob ip-address mac-address type

no arp oob ip-address

Parameter Description

Parameter	Description
ip-address	The IP address corresponding to the MAC address, written as four groups of dotted decimal values.
mac-address	The data link layer address, composed of 48 bits.
type	The ARP encapsulation type. The key word for the Ethernet interface is **arpa**.

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.

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
seconds	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 Examples The following example sets the retry interval of the ARP request as 30 seconds.

```
Ruijie(config)# arp retry interval 30
```

Related Commands

Command	Description
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 Description

Parameter	Description
number	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 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 times of the ARP request smaller. In general, the retry times should not be set too large.

Configuration Examples The following example sets the local ARP request not to be retried.

```
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 Commands

Command	Description
arp retry interval	Interval for retransmitting an ARP request message

Platform Description N/A

2.8 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 Description

Parameter	Description
secondsv	The timeout is in the range from 0 to 2147483 in the unit of seconds.

Defaults The default is 3600.

Command Mode Interface configuration 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 Description N/A

2.9 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
number	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 Description N/A

2.10 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 Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The egress gateway trusted ARP is different from GSN trusted ARP. With this function enabled, the device sends a unicast request for confirmation when learning an ARP table entry. The device learns the ARP table entry after receiving the response. When the device receives the ARP packet, only if the ARP table entry is aged or incomplete and the ARP packet is a response packet will the packet be handled. After egress gateway trusted ARP is enabled, the aging time of the ARP table entry turns to 60 seconds. After this function is disabled, the aging time restores to 3600 seconds.

Configuration Examples The following example enables egress gateway trusted ARP.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp trust-monitor enable
```

The following example disables engress gateway trusted ARP.

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.11 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 Description N/A

2.12 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*

Parameter Description

Parameter	Description
vid1	VID set by the server.
vid2	VID after the transformation.

Defaults This function is disabled by default.

Command Global configuration mode.

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.

```
Ruijie(config)# arp trusted user-vlan 3 translated-vlan 5
```

Related Commands

Command	Description
service trustedarp	Enables the trusted ARP function.

Platform Description N/A

2.13 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 Description

Parameter	Description
number	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 Examples The following example sets the maximum number of the unresolved items to 500.

```
Ruijie(config)# arp unresolve 500
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.14 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 Description

Parameter	Description
trusted	Deletes trusted ARP entries. Dynamic ARP entries are deleted by default.
vrf *vrf_name*	Deletes dynamic ARP entries of the specified VRF instance. The default is the public instance.
ip	Deletes ARP entries of the specified IP address. If *trusted* value is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
mask	Deletes ARP entries in a subnet mask. If *trusted* 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 *interface-name*	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 This command can be used to refresh an ARP cache table.

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 SVI1.

```
Ruijie# clear arp-cache interface Vlan 1
```

Related Commands

Command	Description
arp	Adds a static mapping record to the ARP cache table.

Platform N/A

Description

2.15 clear arp-cache oob

Use this command to clear dynamic ARP mapping records.

clear arp-cache oob [ip [mask]]

Parameter Description

Parameter	Description
ip	Clears the ARP table entriy of the specified IP address. All dynamic ARP table entries are cleared by default.
mask	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 Mode Privileged EXEC 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 Examples The following example clears the cache table of dynamic ARP mapping records.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

2.16 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 Description

Parameter	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

2.17 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 Description

Parameter	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 Examples The following example enables local proxy ARP on VLAN1.

```
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

2.18 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 Description	Parameter	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 N/A

Description

2.19 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.

In the following three cases, the STP protocol clears not only the dynamic MAC address of a port but also the trusted entries, including trusted MAC and trusted ARP:

STP is enabled.

The port is set to neither root port nor designed port. This may be caused when the port is up or down or the port priority is modified.

TC packet is received on the port, and the addresses of the ports not receiving PC packet are cleared.

Configuration Examples The following example enables the trusted ARP function in global configuration mode.

```
config
service trustedarp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.20 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

show arp [[**vrf** *vrf-name*] [**trusted**] *ip* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]

Parameter

Parameter	Description

Description

ip	Displays the ARP entry of the specified IP address.
vrf vrf-name	VRF instance, which Displays the ARP entry with specified VRF.
ip mask	Displays the ARP entries of the network segment included within the mask.
trusted	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
static	Displays all the static ARP entries.
complete	Displays all the resolved dynamic ARP entries.
incomplete	Displays all the unresolved dynamic ARP entries.
mac-address	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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.21 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
ip	Displays ARP table entries of the specified IP address.
mask	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.
mac-address	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 Description N/A

2.22 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

show arp counter

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 output result of the **show arp counter** command:

```
Ruijie# show arp counter
The Arp Entry counter:0
The Unresolve Arp Entry:0
```

The meaning of each field in the ARP cache table is described in Table 1.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

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* | *ip* [*mask*] | *mac-address* | **static | complete | incomplete**]

Parameter Description

Parameter	Description
interface-type interface-number	Displays the ARP of the layer 2 port or the layer 3 interface.
ip	Displays the ARP entry of the specified IP address.
ip mask	Displays the ARP entries of the network segment included within the mask.
mac-address	Displays the ARP entry of the specified MAC address.
static	Displays all the static ARP entries.
completev	Displays all the resolved dynamic ARP entries.
incomplete	Displays all the unresolved dynamic ARP entries.

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.

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
20.1.1.1 000f.e200.0001 Static -- -- --
20.1.1.1 000f.e200.0001 Static -- Vl3 --
20.1.1.1 000f.e200.0001 Static -- Vl3 Gi2/0/1
193.1.1.70 00e0.fe50.6503 Dynamic 1 Vl3 Gi2/0/1
192.168.0.1 0012.a990.2241 Dynamic 10 Gi2/0/3 Gi2/0/3
192.168.0.1 0012.a990.2241 Dynamic 20 Ag1 Ag1
192.168.0.1 0012.a990.2241 Dynamic 30 Vl2 Ag2
192.168.0.39 0012.a990.2241 Local -- Vl3 --
192.168.0.39 0012.a990.2241 Local -- Gi2/0/3 --
192.168.0.1 0012.a990.2241 Local -- Vl3 --
192.168.0.1 0012.a990.2241 Local -- Gi2/3/2 --
```

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.24 show arp packet statistics

Use this command to display the statistics of ARP packets.

show arp packet statistics [*interface-name*]

Parameter Description

Parameter	Description
interface-name	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

2.25 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 Examples The following example displays the output of the **show arp timeout** command:

```
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 Description N/A

2.26 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

show ip arp

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 output of **show ip arp**:

```
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 Description N/A

3 IPv6 Commands

3.1 clear ipv6 neighbors

Use this command to clear the dynamically learned IPv6 neighbors.

clear ipv6 neighbors [**vrf** *vrf-name*] [**oob**] [*interface-id*]

Parameter Description

Parameter	Description
vrf-name	VRF name. All global IPv6 neighbors are cleared without specified VRF name by default.
oob	Clears the dynamically learned IPv6 neighbors discovered by neighbors n MGMT interpface.
interface-id	Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command does not clear all the dynamically learned neighbors on authentication VLAN.
Note that the static neighbors will not be cleared.

Configuration Examples The following example clears the dynamically learned IPv6 neighbors.

```
Ruijie# clear ipv6 neighbors
```

Related Commands

Command	Description
ipv6 neighbor	Configures the neighbor.
show ipv6 neighbors	Displays the neighbor information.

Platform Description N/A

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 Description

Parameter	Description
iipv6-prefix	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.
ipv6-address	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.
prefix-length	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.
prefix-name	The general prefix name. Use the specified general prefix to generate the interface address.
sub-bits	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.
eui-64	The generated IPV6 address consists of the address prefix and the 64 bit interface ID

Defaults N/A

Command Mode Interface configuration 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**.

1.

Configuration Examples

```
Ruijie(config-if)# ipv6 address 2001:1::1/64
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 Description N/A

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 Description	Parameter	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 Examples

```
Ruijie(config-if)# ipv6 address autoconfig default
Ruijie(config-if)# no ipv6 address autoconfig
```

Related Commands	Command	Description
	ipv6 address ipv6-*prefix/prefix-length* [**eui-64**]	Configures the IPv6 address for the interface manually.

Platform Description N/A

3.4 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 Description

Parameter	Description
milliseconds	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.
bucket-size	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 Mode Global configuration 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 Description N/A

3.5 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 Description	Parameter	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**.

Configuration Examples

```
Ruijie(config-if)# ipv6 enable
```

Related Commands	Command	Description
	show ipv6 interface	Displays the related information of an interface.

Platform Description N/A

3.6 Ipv6 gateway

Use this command to configure the default gateway IPv6 address on the management port.

ipv6 gateway *ipv6-address*

Parameter Description

Parameter	Description
ipv6-address	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.

```
Ruijie(config)# interface mgmt 0
Ruijie(config-int)# ipv6 gateway 2001:1::1
Ruijie(config-int)# exit
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 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 Description

Parameter	Description
prefix-name	The general prefix name.
pv6-prefix	The network prefix value of the general-prefix following the format defined in RFC4291.
prefix-length	The length of the general prefix.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide 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.

A general prefix could contain multiple prefixes.

These longer specified prefixes are usually used for the Ipv6 address configuration on the interface.

Configuration Examples The following example configures manually a general prefix as my-prefix.

```
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 Description N/A

3.8 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 Description

Parameter	Description
N/A	N/A

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 Description N/A

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 Description

Parameter	Description
bytes	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 Description

Parameter	Description
value	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
value	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
```

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.

Platform Description N/A

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
	value	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 Description N/A

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 Description	Parameter	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 Examples

```
Ruijie(config-if)# ipv6 nd managed-config-flag
```

Related Commands	Command	Description
	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 Description N/A

3.14 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 Description	Parameter	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 Description N/A

3.15 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 Description

Parameter	Description
milliseconds	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(conifig-if)# ipv6 nd ns-interval 2000
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

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**]]

no ipv6 nd prefix { *ipv6-prefix/prefix-length* | **default** } [[**off-link**] [**no-autoconfig**] | [**no-advertise**]]

Parameter Description

Parameter	Description
ipv6-prefix	IPv6 network ID following the format defined in RFC4291
prefix-length	Length of the IPv6 prefix. "/" shall be added in front of the prefix
valid-lifetime	Valid lifetime of the RA prefix received by the host
preferred-lifetime	Preferred lifetime of the RA prefix received by the host
at valid-date preferred-date	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.

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 Mode Interface configuration 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 Examples The following example adds a prefix for SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(conifig-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 Description N/A

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
value	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 Examples

```
Ruijie(config -if)# ipv6 nd ra-hoplimit 110
```

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 Description N/A

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-interva l

Parameter Description

Parameter	Description
seconds	Interval of sending the RA message in seconds, 3-1800s.
min-max	Maximum and minimum interval sending the RA message in seconds
min_value	Minimum interval sending the RA message in seconds
max_value	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 Mode Interface configuration 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 Examples

```
Ruijie(conifig-if)# ipv6 nd ra-interval 110
Ruijie(config-if)# ipv6 nd ra-interval min-max 110 120
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.
ipv6 nd ra-lifetime	Sets the lifetime of the device.
ipv6 nd ra-hoplimit	Sets the hopfcount of the RA message.
ipv6 nd ra-mtu	Sets the MTU of the RA message.

Platform Description N/A

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 Description

Parameter	Description
seconds	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 Mode Interface configuration 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 Examples

```
Ruijie(conifig-if)# ipv6 nd ra-lifetime 2000
```

Related Commands

Command	Description
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 Description N/A

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 Description

Parameter	Description
value	MTU value, in the range from 0 to 4294967295.

Defaults IPv6 MTU value of the network interface.

Command Mode Interface configuration 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
```

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 Description N/A

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 Description

Parameter	Description
milliseconds	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 Mode Interface configuration 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.

According to RFC4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5*configured value to 1.5*configured value.

Configuration Examples

```
Ruijie(config-if)# ipv6 nd reachable-time 1000000
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

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 stale-time *seconds*

no ipv6 nd stale-time

Parameter Description

Parameter	Description
Seconds	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 Mode Global configuration 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 Commands

Command	Description
N/A	N/A

Platform Description N/A

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 Description	Parameter	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 Commands	Command	Description
	N/A	N/A

Platform Description N/A

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 disable this function.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration 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	Command	Description

Commands	show ipv6 interface	Displays the interface information.

Platform Description N/A

3.25 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 Description

Parameter	Description
number	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 Mode Global configuration mode

Usage Guide This command is used to prevent unresolved ND table entries generated by malicious scan attacks from consuming table entry resources,

Configuration Examples The following example sets the maximum number of the unresolved neighbor table entries to 200.

```
Ruijie(config)# ipv6 nd unresolved 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.26 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		
	ipv6-address	The neighbor IPv6 address, in the form as defined in RFC4291.
	interface-id	Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface).
	hardware-address	The 48-bit MAC address, a dotted triple of four-digit hexadecimal numbers.

Defaults No static neighbor is configured by default.

Command Mode Global configuration 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 Examples The following example configures a static neighbor on SVI 1.

```
Ruijie(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.27 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.28 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 Description

Parameter	Description
N/A	N/A

Defaults The **ipv6 redirects** command is enabled by default.

Command Mode Interface configuration mode.

Usage Guide The transmission rate of any ICMPv6 error message is limited. By default, it is 10pps.

Configuration Examples The following example enables ICMPv6 redirection on interface GigabitEthernet 0/1.
```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 redirects
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

3.29 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 Description

Parameter	Description
N/A	N/A

Defaults The **ipv6 source-route** command is disabled by default.

Command Mode Global configuration 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 Examples

```
Ruijie(config)# no ipv6 source-route
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.30 show ipv6 address

Use this command to display the IPv6 addresses.

show ipv6 address [*interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays all IPv6 address configured on the device.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

3.31 show ipv6 general-prefix

Use this command to display the information of the general prefix.

show ipv6 general-prefix

Parameter Description

Parameter	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 Commands

Command	Description
ipv6 general-prefix	Configures the general prefix.

Platform Description N/A

3.32 show ipv6 interface

Use this command to display the IPv6 interface information.

show ipv6 interface [*interface-id*] [**ra-info**]] [*brief* [interface-id]]

Parameter Description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregate port, or SVI)
ra-info	Displays the RA information of the interface.
brief	Displays the brief information of the interface (interface status and address information).

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.

Configuration Examples The following example displays the information of the IPv6 interface.

```
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.
vltime	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

3.33 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

show ipv6 neighbors [**vrf** *vrf-name*] [**verbose**] [*interface-id*] [*ipv6-address*]

show ipv6 neighbors static

Parameter Description

Parameter	Description
verbose	Displays the neighbor details.
static	Displays the validity status of static neighbors.
vrf-name	VRF name
interface-id	Displays the neighbors of the specified interface.
ipv6-addres	Displays the neighbors of the specified IPv6 address.

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: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. 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. 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. 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). ?: Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.
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	Command	Description

Commands	ipv6 neighbor	Configures a neighbor.

Platform Description N/A

3.34 show ipv6 neighbors statistics

Use the following commands to display the statistics of one IPv6 neighbors.

show ipv6 neighbors [**vrf** *vrf-name*] **statistics**

Use the following command to show the statistics of all IPv6 neighbors.

show ipv6 neighbors statistics all

Parameter Description	Parameter	Description
	vrf-name	VRF name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the statistics of the global neighbors.

```
Ruijie#show ipv6 neighbors statistics
Memory: 1000 bytes
Entries: 10
  Static: 1,Dynamic: 9,Local: 0
  Incomplete:1, Reachable:5, Stale:1, Delay:1, Probe:1

Ruijie#show ipv6 neighbors statistics all
IPv6 neighbor table count: 2
Static neighbor count: 4(2 active, 2 inactive)
Total
  Memory: 2000 bytes
  Entries: 20
    Static: 2,Dynamic: 18,Local: 0
    Incomplete:2, Reachable:10, Stale:2, Delay:2, Probe:2

Global
  Memory: 1000 bytes
  Entries: 10
    Static: 1,Dynamic: 9,Local: 0
    Incomplete:1, Reachable:5, Stale:1, Delay:1, Probe:1

VRF1
  Memory: 1000 bytes
  Entries: 10
    Static: 1,Dynamic: 9,Local: 0
    Incomplete:1, Reachable:5, Stale:1, Delay:1, Probe:1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description Supported on all platforms.

3.35 show ipv6 packet statistics

Use this command to display the statistics of IPv6 packets.

show ipv6 packet statistics [**total** | *interface-name*]

Parameter Description	Parameter	Description
	total	Displays total statistics of all interfaces.
	interface-name	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 inerface.

```
Ruijie#show ipv6 packet statistics
Total
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50

VLAN 1
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50
```

The following example displays the total statistics of the Ipv6 packets.

```
Ruijie#show ipv6 packet statistics total
Received 1000 packets, 1000000 bytes
  Unicast:1000,Multicast:0
  Discards:0
    HdrErrors:0(HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
Sent 100 packets, 6000 bytes
  Unicast:50,Multicast:50
```

Related Commands	Command	Description
	N/A	N/A

Platform Description Supported on all platforms.

3.36 show ipv6 raw-socket

Use this command to display all IPv6 raw sockets.

show ipv6 raw-socket [num **]**

Parameter Description	Parameter	Description
	num	Protocol.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays all IPv6 raw sockets.

```
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 Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.37 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 Description	Parameter	Description
	interface-type interface-number	(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 Examples The following example displays the IPv6 router

```
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 Description N/A

3.38 show ipv6 sockets

Use this command to display all IPv6 sockets.

show ipv6 sockets

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 all IPv6 sockets.

```
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 Description N/A

3.39 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 Examples The following example displays all IPv6 UDP sockets.

```
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 Description

Parameter	Description
low-ip-address	Start address in the network segment range.
high-ip-address	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 AM rule configuration mode.

address-manage

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is configured on the server and should be used together with supervlan.

Configuration Examples The following example enters 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 Description	**Parameter**	**Description**
	file-name	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 Examples The following example defines the device.conf as the startup file name.

```
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 Description N/A

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

Parameter Description

Parameter	Description
class-name	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 Examples The following example configures the address *mypool0* to associate with class1.

```
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 Description N/A

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 Description

Parameter	Description
*	Deletes all DHCP bindings.
ip-address	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 Examples The following example clears the DHCP binding with the IP address 192.168.12.100.

```
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 Description N/A

4.6 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record.

clear ip dhcp conflict { * | *ip-address* }

Parameter Description

Parameter	Description
*	Deletes all DHCP address conflict records.
ip-address	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.

```
clear ip dhcp conflict *
```

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 Description

Parameter	Description
*	Clears all addresses assigned by the DHCP server.
mac-address	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 Examples The following example clears all addresses assigned by the DHCP server.

```
Ruijie# clear ip dhcp history *
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.8 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

4.9 clear ip dhcp relay statistics

Use this command to clear the DHCP relay statistics.

clear ip dhcp relay statistics

Parameter Description

Parameter	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 Examples The following example clears the DHCP relay statistics.

```
Ruijie# clear ip dhcp relay statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.10 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 Description

Parameter	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

4.11 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** form of this command to restore the default setting.

client-identifier *unique-identifier*

no client-identifier

Parameter Description

Parameter	Description
unique-identifier	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 Mode DHCP address pool configuration 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 Description N/A

4.12 client-name

Use this command to define the name of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.

client-name *client-name*

no 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 Mode DHCP address pool configuration 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 Examples The following example defines a string river as the name of the client.

```
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 Description N/A

4.13 default-router

Use this command to define the default gateway of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.

default-router *ip-address* [*ip-address2…ip-address8*]

no default-router

Parameter Description

Parameter	Description
ip-address	Defines the IP address of the equipment. It is required to configure one IP address at least.

ip-address2…ip-address8	(Optional) Up to 8 gateways can be configured.

Defaults No gateway is defined by default.

Command Mode DHCP address pool configuration 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 Examples The following example defines 192.168.12.1 as the default gateway.

```
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 Description N/A

4.14 dns-server

Use this command to define the DNS server of the DHCP client in the DHPC address pool configuration mode. Use the **no** 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

Parameter Description

Parameter	Description
ip-address	Defines the IP address of the DNS server. At least one IP address should be configured.
ip-address2…ip-address8	(Optional) Up to 8 DNS servers can be configured.
use-dhcp-client interface-type interface-number	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 priory, 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 Description N/A

4.15 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.

domain-name *domain-name*

no domain-name

Parameter Description

Parameter	Description
domain-name	Defines the suffix domain name string of the DHCP client.

Defaults No suffix domain name by default.

Command Mode DHCP address pool configuration 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 Examples The following example defines the suffix domain name i-net.com.cn for the DHCP client.

```
domain-name i-net.com.cn
```

Related Commands

Command	Description
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 Description N/A

4.16 hardware-address

Use this command to define the hardware address of the DHCP client in the DHPC address pool configuration mode. Use the **no** form of this command to restore the default setting.

hardware-address *hardware-address* [*type*]

no hardware-address

Parameter Description

Parameter	Description
hardware-address	Define the MAC address of the DHCP client.
type	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 Examples The following example defines the MAC address 00d0.f838.bf3d with the type ethernet.

```
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 Description N/A

4.17 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** form of this command to restore the default setting.

host *ip-address* [*netmask*]

no host

Parameter Description

Parameter	Description
ip-address	Defines the IP address of DHCP client.
netmask	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.

Platform Description N/A

4.18 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** form of this command to restore the default setting.

ip address dhcp

no ip address dhcp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The interface cannot obtain the ID address by the DHCP by default.

Command Mode Interface configuration 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 Examples The following example makes the FastEthernet 0 port obtain the IP address automatically.

```
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 Description N/A

4.19 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 Description	Parameter	Description
	class-name	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 Examples The following example configures a global CLASS.

```
Ruijie(config)# ip dhcp class myclass
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.20 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** 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*]

Parameter Description

Parameter	Description
low-ip-address	Excludes the IP address, or excludes the start IP address within the range of the IP address.
high-ip-address	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

4.21 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. The forcible NAK packet sending function is added to shorten the interval at which the client sends 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

4.22 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** 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

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 Commands

Command	Description
N/A	N/A

Platform Description N/A

4.23 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** form of this command to restore the default setting.

ip dhcp ping packets [*number*]

no ip dhcp ping packets

Parameter Description

Parameter	Description
number	(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 Description N/A

4.24 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** form of this command to restore the default setting.

ip dhcp ping timeout *milli-seconds*

no ip dhcp ping timeout

Parameter Description

Parameter	Description
milli-seconds	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

Defaults The default is 500 seconds.

Command Mode Global configuration mode.

Usage Guide This command defines the time that the DHCP server waits for a ping response packet.

Configuration Examples The following example configures the waiting time of the ping response packet to 600ms.

```
ip dhcp ping timeout 600
```

Related Commands

Command	Description
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 Description N/A

4.25 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** form of this command to restore the default setting.

ip dhcp pool *pool-name*

no ip dhcp pool *pool-name*

Parameter Description

Parameter	Description
pool-name	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 N/A

Description

4.26 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 Description	**Parameter**	**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 Examples The following example enables the ip dhcp relay check server-id function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay check server-id
```

Related Commands	**Command**	**Description**
	service dhcp	Enables the DHCP Relay.

Platform Description N/A

4.27 ip dhcp relay information option82

Use this command to configure 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 This command is exclusive with the **option dot1x** command.

Configuration Examples The following example enables the option82 function on the DHCP relay.

```
Ruijie# configure terminal
Ruijie(config)# Ip dhcp relay information option82
```

Related Commands

Command	Description
service dhcp	Enables the DHCP Relay.

Platform Description N/A

4.28 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 Description

Parameter	Description
N/A	N/A

Defaults The **ip dhcp relay suppression** command is disabled.

Command Mode Interface configuration mode.

Usage Guide After executing this command, the system will not relay the DHCP request message on the interface.

Configuration Examples The following example enables the relay suppression function on the interface 1.

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp relay suppression
Ruijie(config-if)# exit
Ruijie(config)#
```

Related Commands

Command	Description
service dhcp	Enables the DHCP Relay.

Platform Description N/A

4.29 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 Description	**Parameter**	**Description**
	N/A	N/A

Defaults Enabled

Command Mode This function is enabled by defualt.

Usage Guide N/A

Configuration Examples The following example enables the CLASS to allocate addresses.

```
Ruijie(config)# ip dhcp use class
```

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description N/A

4.30 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 [**vrf** *vrf-name*] *A.B.C.D*

no ip helper-address [**vrf** *vrf-name*] *A.B.C.D*

Parameter Description	**Parameter**	**Description**
	N/A	N/A

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

4.31 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

Parameter Description

Parameter	Description
days	Lease time in days
hours	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
minutes	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.
infinite	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 Mode DHCP address pool configuration 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 Examples The following example sets the DHCP lease to 1 hour.

```
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 Description N/A

4.32 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*

defaut lease-threshold

no lease-threshold

Parameter Description

Parameter	Description
percentage	Usage of the address pool, ranging from 60 to 100 in percentage.

Defaults 90

Command Mode DHCP address pool configuration 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 Examples The following example sets the alarm threshold to 80%.

```
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 Description N/A

4.33 match ip

Use this command to define an AM rule. Use the **no** form of this command to remove the configuration.

match ip *ip-address netmask* [*interface*] [**add/remove**] **vlan** *vlan-list*

no match ip *ip-address netmask* [*interface*] [**add/remove**] **vlan** *vlan-list*

Parameter Description

Parameter	Description
ip-address	IP address
netmask	Subnet mask
interface	Interface ID
add/remove	Adds or removes the specified VLAN
vlan-list	VLAN ID

Defaults N/A

Command Mode AM rule configuration mode

Usage Guide With this function enabled, all DHCP clients without VLAN+port/VLAN configuration obtain addresses in the rule.

If the DHCP client obtains a static address in subvlan, he gets the static address in whichever subvlan. The AM rule configuration is based on VLAN and applies to only static addresses.

Configuration Examples The following example defines an AM rule.

```
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 Description N/A

4.34 match ip default

Use this command to define a default AM 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 Description

Parameter	Description
ip-address	IP address
netmask	Subnet mask

Defaults N/A

Command Mode AM rule configuration mode

Usage Guide With this function enabled, all DHCP clients without VLAN+port/VLAN configuration obtain addresses in the default rule.

Configuration Examples The following example defines a default AM 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 Description N/A

4.35 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*]

netbios-name-server

Parameter Description

Parameter	Description
ip-address	IP address of the WINS server. It is required to configure one IP address at least.
ip-address2…ip-address8	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.

Defaults No WINS server is defined by default.

Command Mode DHCP address pool configuration mode.

Usage Guide When more than one WINS server is defined, the former has higher priory. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

Configuration Examples The following example specifies the WINS server 192.168.12.3 for the DHCP client.

```
netbios-name-server 192.168.12.3
```

Related Commands

Command	Description
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 Description N/A

4.36 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** form of this command to restore the default setting.

netbios-node-type *type*

no netbios-node-type

Parameter Description

Parameter	Description
type	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 Mode DHCP address pool configuration 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 Examples The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

```
netbios-node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.
netbios-name-server	Configures the WINS name server of the Microsoft DHCP client NETBIOS.

Platform Description N/A

4.37 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** form of this command to restore the default setting.

network *net-number net-mask*

no network

Parameter Description

Parameter	Description
net-number	Network number of the DHCP address pool
net-mask	Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default.

Defaults No network number or network mask is defined by default.

Command Mode DHCP address pool configuration 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 Description N/A

4.38 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** form of this command to restore the default setting.

next-server *ip-address* [*ip-address2…ip-address8*]

no next-server

Parameter Description

Parameter	Description
ip-address	Defines the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.
ip-address2…ip-address8	(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 priory. 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

Command	Description

Commands		
	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 Description N/A

4.39 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. Use the **no** form of this command to restore the default setting.

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

no option

Parameter Description

Parameter	Description
code	Defines the DHCP option codes.
ascii *string*	Defines an ASCII string.
hex *string*	Defines a hex string.
ip *ip-address*	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 Description N/A

4.40 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 Commands

Command	Description
N/A	N/A

Platform Description N/A

4.41 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 Commands	**Command**	**Description**
	ip dhcp class	Defines a CLASS and enters the global CLASS configuration mode.

Platform Description N/A

4.42 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 Description	**Parameter**	**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

4.43 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 Description

Parameter	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

4.44 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in global configuration mode. Use the **no** form of this command to restore the default setting.

service dhcp

no 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**
	show ip dhcp server statistics	Displays various statistics information of the DHCP server.
	ip helper-address [**vrf**] *A.B.C.D*	Adds an IP address of the DHCP server.

Platform Description N/A

4.45 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 Examples The following example displays the excluded address.

```
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 Description N/A

4.46 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

Command	Description

Commands	N/A	N/A

Platform Description N/A

4.47 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 Description N/A

4.48 show dhcp name

Use this command to display all DHCP address pool names.

show dhcp name

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 all DHCP address pool names.

```
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 Description N/A

4.49 show dhcp pool

Use this command to display the configuration of a specified address pool.

show dhcp pool *name*

Parameter Description	Parameter	Description
	name	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 Description N/A

4.50 show dhcp state

Use this command to display whether DHCP server is enabled.

show dhcp state

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 whether DHCP server is enabled.

```
Ruijie#show dhcp state
```

```
dhcp-server state : true
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

4.51 show ip dhcp binding

Use this command to display the binding condition of the DHCP address.

show ip dhcp binding [*ip-address*]

Parameter Description	Parameter	Description
	ip-address	(Optional) Only displays the binding condition of the specified IP addresses.

Defaults N/A

Command Mode Privileged EXEC 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 Examples The following is the result of the show ip dhcp binding.

```
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 Description N/A

4.52 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 Mode Privileged EXEC mode.

Usage Guide This command can display the conflict address list detected by the DHCP server.

Configuration Examples The following example displays the output result of the **show ip dhcp conflict** command.

```
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 Description N/A

4.53 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
------------  -----------  -----------  -----------  --------
wwp           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 Description N/A

4.54 show ip dhcp pool

Use this command to display the address statistics of an address pool.

show ip dhcp pool [*poolname*]

Parameter Description

Parameter	Description
poolname	(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 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

4.55 show ip dhcp relay-statistics

Use this command to display the statistics of the DHCP relay.

show ip dhcp relay-statistics

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 DHCP relay.

Configuration Examples The following example displays the statistics of the DHCP relay.

```
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 Description N/A

4.56 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.

```
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
DHCPREQTIMES              0
DHCPREQSUCTIMES           0
DISCOVER-PROCESS-ERROR 0
LEASE-IN-PINGSTATE        0
NO-LEASE-RESOURCE         0
SERVERID-NO-MATCH         0
------------------------------------------
recv                      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 Description N/A

4.57 show ip dhcp socket

Use this command to display the socket used by the DHCP server.

show ip dhcp socket

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 socket used by the DHCP server.

```
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 Description

Parameter	Description
ipv6-address	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

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. Use this command to clear the address conflicts.

clear ipv6 dhcp conflict { *ipv6-address* | * }

Parameter Description

Parameter	Description
ipv6-address	Specifiies IPv6 address or prefix.
*	All IPv6 addresses or prefixes.

Defaults N/A

Command Privileged EXEC mode.

Mode

Usage Guide 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 Examples The following example clears a DHCPv6 address conflict.

```
Ruijie# clear ipv6 dhcp conflict 2008:50::2
```

Related Commands

Command	Description
show ipv6 dhcp conflict	Displays address conflicts.

Platform Description N/A

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 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 the packet sending and receiving condition with the DHCPv6 Relay function enabled.

```
Ruijie# clear ipv6 dhcp relay statistics
```

Related Commands

Command	Description
show ipv6 dhcp relay statistics	Displays the statistical information.

Platform Description N/A

5.4 clear ipv6 dhcp server statistics

Use this command to clear the DHCPv6 server statistics.

clear ipv6 dhcp server statistics

Parameter Description

Parameter	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 Examples The following example clears the DHCPv6 server statistics.

```
Ruijie(config)# clear ipv6 dhcp server statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 Description

Parameter	Description
ipv6-address	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 Examples The following example configures the DNS server address.

```
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 Description N/A

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 Description

Parameter	Description
domain	Sets the domain name.

Defaults By default, no domain name is configured.

Command Mode DHCPv6 pool configuration 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 Examples The following example sets the domain name for the DHCPv6 server to example.com.

```
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 Description N/A

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 Description

Parameter	Description
ipv6-prefix/prefix-length	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 *valid-lifetime* amd *preferred-lifetime* shall be configured.
valid-lifetime	Sets the valid lifetime of using the allocated address for the client.
preferred-lifetime	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 Description

Parameter	Description
poolname	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 Examples The following example sets the DHCPv6 server pool.

```
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 Description

Parameter	Description
ipv6-address	Sets the DHCPv6 relay destination address.
interface-type interface-number	Specifies the forwarding output interface if the forwarding address is the local link address.

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 Examples The following example sets the relay destination address on the interface.

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp relay destination 2008:1::1
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays the DHCPv6 interface information.

Platform Description N/A

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 Description

Parameter	Description
poolname	Defines the DHCPv6 pool name.
rapid-commit	Allows the two-message interaction process.
preference *value*	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 Examples The following example enables the DHCPv6 server on the interface.

```
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 Description N/A

5.11 ipv6 local pool

Use this command to configure the local prefix pool of the DHCPv6 server prefix delegation. Use the **no** form of this command to delete the configured local prefix pool.
ipv6 local pool *poolname prefix/prefix-length assigned-length*
no ipv6 local pool *poolname*

Parameter Description

Parameter	Description
poolname	The local prefix pool name.
prefix/prefix-length	The prefix and prefix length.
assigned-length	The assigned prefix length.

Defaults By default, no local prefix pool of the DHCPv6 server prefix delegation 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 Examples The following example configures the local prefix pool.

```
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

Command	Description

Commands	N/A	N/A

Platform Description N/A

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 delete the configured CAPWAP AC IPv6 address.

option52 *ipv6-address*

no option52 *ipv6-address*

Parameter Description	Parameter	Description
	ipv6-address	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 Description N/A

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 Description	Parameter	Description
	ipv6-prefix/prefix-length	Sets the IPv6 address prefix and the prefix length.
	client-DUID	Sets the client DUID.
	lifetime	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 Description

Parameter	Description
poolname	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 *valid-lifetime* and *preferred-lifetime* shall be configured.
valid-lifetime	Sets the valid lifetime of using the allocated address prefix for the client.
preferred-lifetime	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 Examples The following example specifies the local prefix pool for the DHCPv6 server.

```
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 Description N/A

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 / Gloabl configuration mode

Usage Guide The server, client and relay on the same device share a DUID.

Configuration Examples The following example displays the device DUID.

```
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 Description N/A

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
	ipv6-address	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 Examples The following example displays the address binding information for the DHCPv6 server.

```
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 Description N/A

5.17 show ipv6 dhcp conflict

Use this command to display the DHCPv6 address conflicts.

show ipv6 dhcp conflict

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 DHCPv6 address conflicts.

```
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 Description N/A

5.18 show ipv6 dhcp interface

Use this command to display the DHCPv6 interface information.

show ipv6 dhcp interface [*interface-name*]

Parameter Description	Parameter	Description
	interface-name	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 Examples The following example displays the DHCPv6 interface information.

```
Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
```

```
Server pool dhcp-pool
Rapid-Commit: disable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.19 show ipv6 dhcp pool

Use this command to display the DHCPv6 pool information.

show ipv6 dhcp pool [*poolname*]

Parameter Description	Parameter	Description
	poolname	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 Examples The following example displays the DHCPv6 pool information.

```
Ruijie# show ipv6 dhcp pool
DHCPv6 pool: dhcp-pool
  DNS server: 2011:1::1
  DNS server: 2011:1::2
  Domain name: example.com
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.20 show ipv6 dhcp relay destination

Use this command to display the destination information about DHCPv6 Relay Agent.

show ipv6 dhcp relay destination

Parameter description

Parameter	Description
all	Displays information about all configured destination addresses and relay exits.
interface *interface-type interface-number*	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 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 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 Description

Parameter	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 Examples The following example displays the DHCPv6 server statistics.

```
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 Description N/A

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
poolname	The local prefix pool name.

Defaults N/A

Command Mode Privileged EXEC 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.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

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
host-name	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 Description N/A

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 Description N/A

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
host-name	The host name of the equipment
ip-address	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 Commands

Command	Description

show hosts	Show the DNS related configuration information.

Platform Description N/A

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 { *ip-address* | *ipv6-address* }

no ip name-server [*ip-address* | *ipv6-address*]

Parameter Description

Parameter	Description
ip-address	The IP address of the domain name server.
ipv6-address	The IPv6 address of the domain name server.

Defaults N/A

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
Ruijie(config)#      ip      name-server      2001:0DB8::250:8bff:fee8:f800
2001:0DB8:0:f004::1
```

Related Commands

Command	Description
show hosts	Displays the DNS related configuration information.

Platform Description N/A

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
host-name	The host name of the equipment
ipv6-address	The IPv6 address of the equipment

Defaults N/A

Command Mode Global configuration mode.

Usage Guide To delete the host list, use the **no ipv6 host** *host-name ipv6-address* command.

Configuration Examples The following example configures the IPv6 address for the domain name.

```
Ruijie(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

Related Commands

Command	Description
show hosts	Displays the DNS related configuration information.

Platform Description N/A

6.6 show hosts

Use this command to display DNS configuration.

show hosts [*hostname*]

Parameter Description

Parameter	Description
hostname	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 Examples

```
Ruijie# show hosts
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
Ruijie(config)#  ftp-server enableThe 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
time	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 login times

Parameter Description

Parameter	Description
time	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 password

Use this command to set the login password for the FTP server. Use the **no** form of this command to restore the default setting.

ftp-server password [*type*] *password*

no ftp-server password

Parameter Description

Parameter	Description
type	Defines the encryption type of the password: 0 or 7. The default type is 0. 0 indicates the password is not encrypted. 7 indicates the password is encrypted.
password	The login password for the FTP server.

Defaults No password is configured by default.

Command Mode Global configuration mode.

Usage Guide For the FTP server, the login username and the login password must be configured to verify the client connection. One password can be set at most.
The password must include the letter or number. The space in front of / behind the password is allowed, but it is ignored. While the space in the middle of the password is a part of password.
The minimum and maximum lengths of the plain-text password are 1 character and 25 characters.
The minimum and maximum lengths of the encrypted password are 4 characters and 52 characters respectively.
The encrypted password is generated by plain-text password encryption and its format must comply with the encryption specification. If the encrypted password is used for the setting, the client must use the corresponding plain-text password for the purpose of successful login.

⚠ Null password is not supported by the FTP server. Without the password configuration, the client fails to pass the identity verification of the server.

Configuration Examples The following example sets the plain-text password to pass:

```
Ruijie(config)# ftp-server password pass
```

The following example sets the cipher-text password to 8001:

```
Ruijie(config)# ftp-server password 7 8001
```

The following example restores the default setting:

```
Ruijie(config)# no ftp-server password
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.5 ftp-server timeout

Use this command to set the FTP session idle timeout. Use the **no** form of this command to restore the default setting.
ftp-server timeout *time*
no ftp-server timeout

Parameter Description

Parameter	Description
time	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 Examples The following example sets the session idle timeout to 5 mimutes:

```
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 Description N/A

7.6 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** form of this command to restore the default setting.

ftp-server topdir *directory*

no ftp-server topdir

Parameter Description

Parameter	Description
directory	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 Examples The following example enables the FTP Server and confines the FTP client access to the syslog 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

7.7 ftp-server username

Use this command to set the login username for the FTP server. Use the **no** form of this command to restore the default setting.

ftp-server username *username*

no ftp-server username

Parameter Description

Parameter	Description
username	Sets the login username.

Defaults No username 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 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
```

The following example restores the default setting:

```
Ruijie(config)# no ftp-server username
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.8 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 control connection is set up or not (the related IP, Port are shown)

The data connection is set up or not (the related IP, Port and the working mode are shown)

The current file transmission type

The login username and password

The FTP server top directory

The session idle timeout setting

Configuration Examples The following example displays the related status information of the FTP server:

```
Ruijie# show ftp-server
ftp-server information
=====================================
enable : Y
topdir : /
timeout: 20min
username config : Y
password config : Y
```

```
type: BINARY
control connect : Y
ftp-server: ip=192.167.201.245  port=21
ftp-client: ip=192.167.201.82  port=4978
port data connect : Y
ftp-server: ip=192.167.201.245  port=22
ftp-client: ip=192.167.201.82  port=4982
passive data connect : N
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8 FTP Client Commands

8.1 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
username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
dest-address	IP address of the target FTP Server.
remote-directory	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.
remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
local-directory	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.
local-file	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

8.2 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
username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
dest-address	IP address of the target FTP Server.
remote-directory	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.
remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
local-directory	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.
local-file	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration Examples 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".

```
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 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**

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 This command is used to configure the file transfer mode to ASCII mode.

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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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**

Parameter Description

Parameter	Description
vrf *vrf-name*	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.

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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.5 ftp-client source-address

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.

ftp-client [**vrf** *vrfname*] **source-address** { *ip-address* | *ipv6-address* }

no ftp-client [**vrf** *vrfname*] **source-address**

Parameter Description

Parameter	Description
vrf *vrf-name*	VRF name. The default is the public network instance.

Defaults By default, the client will not bind the IP address locally. Instead, the router will select the IP address.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example binds FTP Client with source IP address 192.168.23.236.

```
Ruijie (config)# ftp-client source-address 192.168.23.236
```

The following example binds FTP Client with source IP address 2003:0:0:0::2.

```
Ruijie(config)# ftp-client source-address 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-address 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-address 2003:0:0:0::2
```

The following example disables source IP address binding.

```
Ruijie(config)# no ftp-client source-address
```

The following example disables source IP address binding.

```
Ruijie(config)# no ftp-client vrf vrf-name source-address
```

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
number	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#show interfaces 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 ipip
  Tunnel transport VPN is no set
Ruijie#show interface tunnel 2
// Here is the public information about the interface
Tunnel attributes:
  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 gre ip
    Key 0x2, Sequencing disabled
    Checksumming of packets enabled
Tunnel transport VPN is vrf_tunnel
```

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 hoplimit 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 filed 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 filed 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 chip entries. 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 show tunnel kernel

Use this command to display configuration information of the tunnel kernel, which is mainly for debugging.

show tunnel kernel [tunnel *number***]**

Parameter Description

Parameter	Description
tunnel *number*	Specifies the tunnel interface number. Otherwise, configuration information of all tunnel ports is displayed by default.

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

Usage Guide This command is used to display configuration information of the tunnel kernel. It is mainly for debugging, excluding the situation where the number of tunnel processes is not in line with the one of kernel. In the case of telnet, before applying this interface, monitor debugging information switch should be turned on.

Configuration Examples The following example displays the number of configured tunnel interfaces.

```
EG1000M(config-if-Tunnel 1)#show tunnel kernel
EG1000M(config-if-Tunnel 1)#*Jul  9 18:43:55: %7: show tunnelk total vsd's tunnel
*Jul  9 18:43:55: %7: **************vsd 0**************
*Jul  9 18:43:55: %7: tun_cnt: 1
```

```
*Jul  9 18:43:55: %7: is_reg_decap: 1
*Jul  9 18:43:55: %7:  >Tunnel num: 1
*Jul  9 18:43:55: %7:  up or down: down
*Jul  9 18:43:55: %7:  Tunnel ifindex: 11
*Jul  9 18:43:55: %7:  Tunnel mode: 6
*Jul  9 18:43:55: %7:  Tunnel is_reg_encap: 1
*Jul  9 18:43:55: %7:  Tunnel rg_intf: a800000417294380
*Jul  9 18:43:55: %7:  Tunnel source family: 2
*Jul  9 18:43:55: %7:    src_ipv4=0.0.0.0
*Jul  9 18:43:55: %7:    src_ipv6=0000:0000:0000:0000:0000:0000:0000:0000
*Jul  9 18:43:55: %7:  Tunnel dest family: 2
*Jul  9 18:43:55: %7:    dst_ipv4=0.0.0.0
*Jul  9 18:43:55: %7:    dst_ipv6=0000:0000:0000:0000:0000:0000:0000:0000
*Jul  9 18:43:55: %7:  Tunnel en key: false
*Jul  9 18:43:55: %7:    key=0
*Jul  9 18:43:55: %7:  Tunnel en check: 0
*Jul  9 18:43:55: %7:  Tunnel gre hdr len: 4
*Jul  9 18:43:56: %7:  Tunnel srclen: 0
*Jul  9 18:43:56: %7:  Tunnel en tos: false
*Jul  9 18:43:56: %7:    tos=0
*Jul  9 18:43:56: %7:  Tunnel en ttl: false
*Jul  9 18:43:56: %7:    ttl=254
*Jul  9 18:43:56: %7:  Tunnel self vrf id: 0
*Jul  9 18:43:56: %7:  Tunnel vrf idx: 0
*Jul  9 18:43:56: %7:  Tunnel 6rd prefix: 0000:0000:0000:0000:0000:0000:0000:0000
*Jul  9 18:43:56: %7:  Tunnel 6rd prefixlen: 0
*Jul  9 18:43:56: %7:  Tunnel 6rd br address: 0.0.0.0, br prefixlen: 0, br suffixlen 0
*Jul  9 18:43:56: %7:  Tunnel is dirty: 0
*Jul  9 18:43:56: %7:  Tunnel pmtud enable: 0
*Jul  9 18:43:56: %7:  Tunnel pmtud learned mtu: 0
*Jul  9 18:43:56: %7:  Tunnel keepalive enable: 0
*Jul  9 18:43:56: %7:  Tunnel recv keepalive flag: 0
*Jul  9 18:43:56: %7:  Tunnel ipsec profile enable: 0
*Jul  9 18:43:56: %7:  Tunnel ipsec profile tun_id[0]: -1
*Jul  9 18:43:56: %7:  Tunnel ipsec profile tun_id[1]: -1
*Jul  9 18:43:56: %7:
*Jul  9 18:43:56: %7: total tunnelk count 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.4 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
ip-address	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 sets the destination IP address of tunnel interface 0 to 61.154.101.3.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel destination 61.154.101.3
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

9.5 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	GRE for the route at the IP layer
gre ipv6	GRE for the route at the IPv6 layer
ipv6	IPv6 network for transmission. No GRE encapsulation.

ipip	IP over IP encapsulation mode
ipv6ip	IPv6 over IP encapsulation mode
ipv6ip 6to4	IPv4 network for transmission. No GRE encapsulation. It is often used to connect the IPv6 network.
ipv6ip isatap	IPv4 network for transmission. No GRE encapsulation. It is often used to deploy the IPv6 network fast for the campus network.

Defaults For routers, the default encapsulation mode is GRE IP.
For switches, the default encapsulation mode is IPv6 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 Examples The following example encapsulates GRE IP on tunnel interface 0.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

9.6 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 { ipv4-address|ipv6-address | interface-type interface-number }

no tunnel source

Parameter Description

Parameter	Description
ipv4-address	Source IPv4 address of the tunnel used as the source IP address of the packets to be transmitted through the tunnel.
ipv6-address	If the tunnel mode ipv6 or tunnel mode gre ipv6 is configured, the source address of the tunnel shall be the IPv6 address. Using the local address of the link as the source address is not supported currently.
interface-type interface-number	Interface referenced by the tunnel, which will be used as the source IPv4 address of the packets to be transmitted through the tunnel.

Defaults No tunnel source address is configured by default.

Command Mode Interface configuration mode.

Usage Guide The source IP address of a tunnel can be a specified IPv4 address or an IPv4 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 Examples The following example configures an IPv6 manual tunnel.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel mode ipv6ip
Ruijie(config-if)# tunnel source vlan 1
Ruijie(config-if)# tunnel destination 192.168.5.1
```

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 Description N/A

9.7 tunnel tos

Use this command to set the IPv4 ToS byte or IPv6 traffic class 8 bits fin tunnel intefface configruation mode. Use the **no** form of this command to restore the default setting.
tunnel tos [*num*]
no tunnel tos

Parameter Description

Parameter	Description
num	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 Interface configuration mode

Mode

Usage Guide T 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 20 on interface tunnel 1.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel tos 20
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

9.8 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 *value*
no tunnel ttl

Parameter Description

Parameter	Description
value	TTL value

Defaults The default is 128.

Command Mode Interface configuration mode.

Usage Guide This command is used to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages.

Configuration Examples

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel ttl 64
```

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 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* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**]]

Parameter Description

Parameter	Description
oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
vrf-name	VRF name
address	Specifies an IPv4 address.
length	Specifies the length of the packet to be sent (range: 36-18024, default: 100).
times	Specifies the number of packets to be sent (range:1-4294967295).
seconds	Specifies the timeout time (range: 1-10 seconds).
data	Specifies the data to fill in.
source	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.

Defaults Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

Command Mode Privileged EXEC mode.

Usage Guide The ping command can be used in the ordinary user mode and the privileged EXEC mode. In the ordinary mode, only the basic functions of ping are available. In the privileged EXEC mode, in addition to the basic functions, the extension functions of the ping are also available. For the ordinary functions of ping, five packets of 100Byte in length are sent to the specified IP address within the specified period (2s by default). If response is received, '!' is displayed. If no response is received, '.' displayed, and the statistics is

displayed at the end. For 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.

Configuration Examples The following example tests the connectivity of a network to locate the network connectivity problem.

```
Ruijie# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, 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 example below shows the extension ping.
Ruijie# ping 192.168.5.197 length 1500 ntimes 100 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds, data
ffff source 192.168.4.10:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.2 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* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**]]

Parameter Description

Parameter	Description
oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
vrf-name	VRF name

Ip-address	Specifies an IPv6 address.
length	Specifies the length of the packet to be sent (range: 36-18024, default: 100).
times	Specifies the number of packets to be sent (range:1-4294967295).
seconds	Specifies the timeout time (range: 1-10 seconds).
data	Specifies the data to fill in.
source	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.

Defaults Five packets with 100Byte in length are sent to the specified IP address within specified time 2s by default

Command Mode Privileged EXEC mode.

Usage Guide The ping ipv6 command can be used in the ordinary user mode and the privileged EXEC mode. In the ordinary mode, only the basic functions of ping ipv6 are available. In the privileged EXEC mode, in addition to the basic functions, the extension functions of the ping ipv6 are also available. For the ordinary functions of ping ipv6, five packets of 100Byte in length are sent to the specified IP address within the specified period (2s by default). If response is received, '!' is displayed. If no response is received, '.' displayed, and the statistics is displayed at 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.

Configuration Examples The following example tests the connectivity of a network to locate the network connectivity problem.

```
Ruijie# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, 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 example below shows the extension ping ipv6.
Ruijie# ping  ipv6 2000::1  length 1500 ntimes 100 timeout 3 data ffff source
192.168.4.10:
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
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

10.3 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**] [*adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

Parameter Description

Parameter	Description
oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
vrf-name	VRF name
address	Specifies an IPv4 address.
number	Specifies the number of probe packets to be sent (range: 1-255).
source	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.
seconds	Specifies the timeout time (range: 1-10 seconds).
minimum maximum	Specifies the minimum and maximum TTL values (range:1-255).

Defaults By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

Command Mode Privileged EXEC mode: enables extended functions.
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 bout 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 Description N/A

10.4 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* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

Parameter Description

Parameter	Description
oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
vrf-name	VRF name
address	Specifies an IPv6 address.
number	Specifies the number of probe packets to be sent.
seconds	Specifies the timeout time.
minimum maximum	Specifies the minimum and maximum TTL values.

Defaults By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

Command Mode Privileged EXEC mode: enables extended functions.
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 bout 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*]

no ip tcp keepalive

Parameter Description

Parameter	Description
interval *num1*	The interval of sending the keepalive packet, in the range from1 to 120 in the unit of seconds, The default is 75.
times *num2*	Keepalive packet sending times, in the range from 1 to 10. The default is 6.
idle-period *num3*	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 1800 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** to180 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 When you run the RGOS 10.x command **service tcp-keepalives-in** or **service tcp-keepalives-out**, it is converted to this command automatically in RGOS 11.0.

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
max-segment-size	Upper limit of the MSS value in the range from 68 to 10000 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 1300 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 *minutes*	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 untill the PMTU value reaches the MSS or the user stops this timer. Use the parameter **age-timer infinite** to stop this timer.

Configuration Examples The following example enables PMTU discovery.

```
Ruijie(config)# ip tcp path-mtu-discovery
```

Related Commands

Command	Description
show tcp pmtu	Shows the PMTU value for the TCP connection.

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	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 The **ip tcp not-send-rst** command in RGOS 10.x is compatible in RGOS 11.0. When you run this command, it is converted to the **no ip tcp send-reset** command automatically.

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
seconds	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 synwait-time 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
size	Size of receiving buffer and sending buffer for TCP connections in the range from 128 to 65535 << 14 bytes.

Defaults The default is 65535.

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.

The sending buffer is used to buffer the data of application programs. Each byte in the sending buffer has a sequence number, and bytes with sequence numbers acknowledged will be removed from the sending buffer. Increasing the sending buffer will improve the interaction between TCP and application programs, thus enhancing the performance. However, increasing the receiving buffer and sending buffer will result in more memory consumption of TCP.

This command is used to change the size of receiving buffer and sending buffer for TCP connections. This command changes both the receiving buffer and sending buffer, and only applies to subsequent connections. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example sets the TCP window size to 16386 bytes.

```
Ruijie(config)# ip tcp window-size 16386
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
interval	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**]

no service tcp-keepalives-out

Parameter Description

Parameter	Description
interval	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 IPv6 address
local-port *num*	Local port

peer-ipv6 *X:X:X:X::X*	Peer IPv6 address
peer-port *num*	Peer port
statistics	Displays IPv6 TCP connection statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv6 TCP connection information.

```
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 Description N/A

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 *X:X:X:X::X*	Local IPv6 address
local-port *num*	Local port
peer-ipv6 *X:X:X:X::X*	Peer IPv6 address
peer-port *num*	Peer port

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example information about IPv6 TCP PMTU.

```
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

Parameter	Description

Description

num	Port number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv6 TCP port status.

```
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 *a.b.c.d*	Local IP address.
local-port *num*	Local port.
peer-ip *a.b.c.d*	Peer IP address.
peer-port *num*	Peer port.
statistics	Displays IPv4 TCP connection statistics.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv4 TCP connection information.

```
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 Description N/A

11.13 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 *num*	Local port.
peer-ip *a.b.c.d*	Peer IP address.
peer-port *num*	Peer port.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays PMTU of IPv4 TCP connection.

```
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 Description N/A

11.14 show tcp port

Use this command to display information about the current TCP port.

show tcp port [*num*]

Parameter Description

Parameter	Description
num	Port number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current IPv4 TCP port status.

```
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	Status of the current 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. 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.

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 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 IPv4 REF packet statistics.

```
Ruijie #clear ip ref packet statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.2 clear ipv6 ref packet statistics

Use this command to clear IPv6 REF packet statistics.

clear 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 Examples The following example clears IPv6 REF packet statistics.

```
Ruijie #clear ipv6 ref packet statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

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 Description	Parameter	Description
	glean	Aggregate adjacent node, which is used for a direct route
	local	Local adjacent node, which is used by the local host
	ip	Next-hop IP address
	interface_type	Interface type
	interface_number	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 Examples The following example displays the information about all adjacent nodes in the adjacent node table.

```
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 Description N/A

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.
source_ipaddress	Source IP address of the packet
dest_ipaddress	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 Examples The following example displays IPv4 REF packet statistics.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

12.6 show ip ref resolve-list

Use this command to display the IPv4 REF resolution information.

show ip ref resolve-list

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 IPv4 REF resolution information.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

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 *vrf_name*	VRF name, supported only by the VRF-supported device.
default	Specifies the default route.
ip	Specifies the destination IP address of the route
mask	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 Commands

Command	Description
show ip ref exact-route	Displays the accurate REF forwarding path of an IP packet.

Platform Description N/A

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 Description

Parameter	Description
glean	Aggregate adjacent node, which is used for a direct route
local	Local adjacent node, which is used by the local host
ipv6-address	Next-hop IP address
interface_type	Interface type
interface_number	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 Examples The following example displays the information about the IPv6 adjacent node..

```
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	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 Description N/A

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 Privileged EXEC mode

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 Description N/A

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 Examples The following example displays IPv6 REF packet statistics.

```
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 Description N/A

12.11 show ipv6 ref resolve-list

This command is used to display the IPv6 REF resolution information.

show ipv6 ref resolve-list

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 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 *vrf_name*	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::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 Examples The following example displays all the routing information in the REF IPv6 table.

```
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 Configuration 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 *vrf-name*	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 Description N/A

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 Examples The following example disables automatic route summary of RIPv2.

```
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 Description N/A

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 **bfd all-interfaces** in the routing progress configuration mode.

Configuration Examples N/A

Related Commands

Command	Description
route ip	Creates the RIP routing progress 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 Description N/A

1.4 default-information originate

Use this command to generate a default route in the RIP progress. 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 *metric-value*	(Optional) The original metric value of the default route with the value range 115 of metric-value.
route-map *map-name*	(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 Examples

The following example generates a default route to the RIP routing table.

```
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 Description N/A

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
metric-value	Indicates the default metric value with the range from 1 to 16. If the metric value is greater than or equal to 16, the RGNOS 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 Description N/A

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
distance	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
ip-address	Indicates the prefix of the source IP address of the route.
wildcard	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 Examples The following example sets the management distance of the RIP route to 160, and specifies the 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 Description N/A

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
access-list-number | *name*	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
prefix *prefix-list-name*	Uses the prefix list to filter the routes.
gateway *prefix-list-name*	Uses the prefix list to filter the source of the routes.
interface-type interface-number	(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
access-list-number | *name*	Specifies the ACL.
prefix *prefix-list-name*	Uses the prefix list to filter routes.
interface	(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 [*area-tag*]	(Optional) Applies route update advertisement control to only routes introduced from ISIS in this distribution list. *area-tag* specifies an ISIS instance.
ospf *process-id*	(Optional) Applies route update advertisement control to only routes introduced from OSPF in this distribution list. *process-id* 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 Examples The following example advertises only the 192.168.12.0/24 route.

```
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 Description N/A

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 Examples The following example operates the RIP instance of a specified VRF, vpn1.

```
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 Examples The following example enters or exits the address family configuration mode.

```
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 Description N/A

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
route-map-name	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 Examples The following example enables FRR for RIP instance 1 and associates route map *fast reroute*.

```
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 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 Description

Parameter	Description
name-of-keychain	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

1.13 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 Examples The following example configures the RIP authentication mode on the fastEthernet 0/1 as MD5.

```
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 Description N/A

1.14 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.

password-string	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 Description N/A

1.15 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.
bdf all-interfaces	Configures all interfaces running RIP to use the BFD to perform link detection.

Platform Description N/A

1.16 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 *metric-value*	Specifies the metric value of the default route, in the range from1 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 Examples The following example creates a default route which is notified on ethernet0/1 only.

```
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 Description N/A

1.17 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 Examples The following example prohibits receiving RIP data packages on fastEthernet 0/1.

```
Ruijie (config)# interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# no ip rip receive enable
```

Related

Command	Description

Commands

ip rip send enable	Enables or disables the interface to send RIP data packages.
passive-interface	Configures a passive RIP interface.

Platform Description N/A

1.18 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 Examples The following example enables receiving both RIPv1 and RIPv2 data packages.

```
Ruijie (config)#interface fastEthernet 0/1
Ruijie (config-if-FastEthernet 0/1)# ip rip receive version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interface.

Platform Description N/A

1.19 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 Examples The following example prohibits sending RIP data packages on fastEthernet 0/1.

```
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 Description N/A

1.20 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 Examples The following example disables sending RIP supernet routes on the fastEthernet 0/1 interface.

```
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 Description N/A

1.21 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 Description N/A

1.22 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 Examples The following example disables the RIP split horizon function on the interface fastethernet 0/0.

```
Ruijie (config)# interface fastethernet 0/0
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 Description N/A

1.23 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
ip-address	Indicates the IP addresses to be converged.
ip-network-mask	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 Description N/A

1.24 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 *timer*	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 *count*	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 Examples The following example enables TRIP and sets the retransmission interval and maximum 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 Description N/A

1.25 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 Examples The following example sends RIPv2 packets in broadcast mode on the fastEthernet 0/1 interface.

```
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 Description N/A

1.26 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
ip-address	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 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
passive-interface	Configures the interface as a passive interface.

Platform Description N/A

1.27 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
network-number	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.
wildcard	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

1.28 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
access-list-number	*name*	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.
offset	Indicates the offset of changed metric values. The value is in the range from 0 to16.
interface-type	Applies the ACL to a specified interface.
interface-number	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 Examples The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7.

```
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 Description N/A

1.29 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 Description

Parameter	Description
delay	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 Routing process configuration mode

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 Examples The following example sets the delay to send RIP update packets to 30 milliseconds.

```
Ruijie(config)# router rip
Ruijie(config-router)# output-delay 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.30 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.
interface-type interface-num	Indicates the interface type and number.

Defaults Interfaces are set to the non passive interfaces by default.

Command Mode Routing process configuration 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 Description N/A

1.31 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** { i**nternal** | **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 *area-tag*	Is redistributed from ISIS and specifies an ISIS instance through area-tag.
ospf *process-id*	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 *metric-value*	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 *route-map-name*	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 Examples The following example redistributes static routes to RIP.

```
Ruijie(config-router)# redistribute static
```

Related Commands

Command	Description
default-metric *metric*	Sets the default metric of the route to be redistributed.
default-information originate	Generates the default route in the RIP process.

Platform Description N/A

1.32 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 Description N/A

1.33 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 Description N/A

1.34 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.
network-number	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
network-mask	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 Examples The following example displays all converged address entries in the RIP routing database.

```
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 Description N/A

1.35 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 Examples The following example displays direct routes redistributed by the RIP process.

```
Ruijie# show ip rip external connected
Protocol connected route:
[connected] 1.0.0.0/8 metric=0
nhop=0.0.0.0, if=2
[connected] 3.0.0.0/8 metric=0
nhop=0.0.0.0, if=16391
[connected] 4.4.0.0/16 metric=0
nhop=0.0.0.0, if=16388
[connected] 5.0.0.0/8 metric=0
nhop=0.0.0.0, if=16386
[connected] 192.168.195.0/24 metric=0
nhop=0.0.0.0, if=1
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.
ip vrf	Creates a VRF.

Platform Description N/A

1.36 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 Examples The following example displays the RIP interface information.

```
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: Registed
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: Registed
    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 Description N/A

1.37 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
ip-address	(Optional) Displays the IP address of a specified RIP neighbor.
vrf *vrf-name*	(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 Examples The following example displays the RIP neighbor information.

```
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 Description N/A

1.38 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
update	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.
invalid	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.
flush	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 Examples The following example enables the RIP update packets that are sent every 10 seconds. If no update 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

1.39 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 Examples The following example disables verification of the source IP address of the update packet.

```
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 Description N/A

1.40 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 Routing process configuration mode

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 Examples The following example configures the RIP version as version 2.

```
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 Description N/A

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
area-id	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 Examples The following example removes the configuration of OSPF area 2.

```
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 Description N/A

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
area-id	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 0when 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 Description N/A

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
area-id	ID of the stub area or NSSA
cost	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
area-id	Area ID
acl-name	Name of an Access Control List (ACL)
prefix-name	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 Examples The following example sets area 1 to learn only the inter-area routes of 172.22.0.0/8.

```
Ruijie # configure terminal
Ruijie(config)# access-list 1 permit 172.22.0.0/8
Ruijie(config)# router ospf 100
Ruijie(config-router)# area 1filter-list access1in
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
area-id	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 *value*	Sets the metric of the generated default LSA. The range is from 0 to 16777214. The default value is 1.
metric *value*	Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
metric-type *type*	Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
translator	Configures the translator for the NSSA ABR.
stability-interval *seconds*	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 Examples The following example sets area 1 as an NSSA on all routers of the area.

```
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 Description N/A

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**] [c**ost** *cost*]
no area *area-id* **range** *ip-address net-mask* [cost]

Parameter Description

Parameter	Description
area-id	ID of the area where the aggregate route is injected into. The value can be a decimal integer or an IP address.
ip address net-mask	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 Examples The following example aggregate the routes of area 1 into a route 172.16.16.0/20.

```
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 Description N/A

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
area-id	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 Examples The following example sets area 1 as the stub area on all devices in area 1.

```
Ruijie(config)# router ospf1
Ruijie(config-router)# network172.16.0.0 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 Description N/A

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*] [**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 Description

Parameter	Description

area-id	ID of the OSPF transition area. The value can be a decimal integer or an IP address.
router-id	ID of the router neighboring to the virtual link. It can be viewed with the show ip ospf command.
dead-interval *seconds*	(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.
hello-interval *seconds*	(Optional)Defines the interval at which the HELLO packet is sent by the OSPF to the virtual link in seconds. The range is from1 to 65535.This value must be consistent with that of the neighbor.
retransmit-interval *seconds*	(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 *seconds*	(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]*key*	(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 *key-id***md5 [0|7]***key*	(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 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.

Configuration Examples The following example sets area 1 as the transition area to establish virtual link with neighbor *2.2.2.2.*

```
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 inMD5 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
```

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 Description N/A

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
ref-bw	Reference bandwidth, in the range from1 to 4294967 Mbps.

Defaults The default is 100Mbps.

Command Mode Routing process configuration mode

Usage Guide This command sets the reference bandwidth for automatically generating the interface cost. Without the optional parameter, the command enables the auto-cost function with the default reference bandwidth. With the optional parameter, the command enables the auto-cost function with a specified reference bandwidth. Note that the **default auto-cost** command enables the auto-cost function with the default configuration, while and the **no auto-cost** command disables the function.
The cost set with the **ip ospf cost** command will replace the auto-cost.

Configuration Examples The following example configures the reference bandwidth as 10 Mbps.

```
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 Description N/A

2.10 bdf 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.
bdf all-interfaces
no bdf 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 Examples N/A

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 Description N/A

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 Examples The following example disables Opaque LSA capability.

```
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 Description N/A

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
process-id	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 Examples The following example clears data of OSPF instance 1 and restarts OSPF instance 1.

```
Ruijie#clearipospf1process
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 Examples The following example determines the best route with the RFC 2328 rule.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# nocommpatiblerfc1583
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information

Platform Description N/A

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*]

[**metric-type 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 *metric*	(Optional) Initial metric of the default route in the range from0 to 16777214
metric-type *type*	(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 *map-name*	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 Mode Routing process configuration 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.
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
metric	Default metric of the OSPF redistribution route in the range from1 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 Examples The following example configures the default metric of the OSPF redistribution route as 50.

```
Switch(config)# router rip
Ruijie(config-router)# network192.168.12.0
Switch(config-router)# version 2
Ruijie(config-router)# exit
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.10.0 0.0.0.255area0
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 Examples The following example disables adding the discard routes generated with the area range command.

```
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 Description N/A

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
distance	Sets the route AD in the range from1 to 255.
intra-area *distance*	Sets the AD of the intra-area route in the range from1 to 255.
inter-area *distance*	Sets the AD of the inter-area route in the range from1 to 255.
External *distance*	Sets the AD of the external route in the range from1 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

Routing process configuration mode

Usage Guide

This command is used to specify different ADs for different types of OSPF routes.

Configuration Examples

The following example sets the OSPF external route AD to 160.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# distance ospf external 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

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

access-list-number | **name**	Uses the ACL filtering rule.
gateway *prefix-list-name*	Uses the gateway filtering rule.
Prefix *prefix-list-name*	Uses the prefix-list filtering rule.
route-map *route-map-name*	Uses the route-map filtering rule.
interface-type interface-number	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

Configuration Examples The following example configures LSA filtering.

```
Ruijie(config)# access-list3permit172.16.0.00.0.127.255
Ruijie(config)# router ospf 25
Ruijie(config-router)# redistribute rip metric100
Ruijie(config-router)# distribute-list 3 in ethernet 0/1
```

Related Commands

Command	Description
distribute-list out	Filters redistribution routes.

Platform Description N/A

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
access-list-number | name	Uses the ACL filtering rule.
prefix prefix-list-name	Uses the prefix-list filtering rule.
bgp | connected | isis [area-tag] **| ospf** process-id| **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 Examples The following example filters the redistributed static routes.

```
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 Examples The following example operates OSPFv2 process 100 over SNMP:

```
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 Description N/A

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** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange** | **VirtNbrStateChange**]]
no enable traps [**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change** [**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** |

NssaTranslatorStatusChange | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange | VirtNbrStateChange**]]

Parameter Description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>error</td><td>Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches.
<table>
<tr><td>Ifauthfailure</td><td>Interface authentication error</td></tr>
<tr><td>Ifconfigerror</td><td>Interface parameter configuration error</td></tr>
<tr><td>Ifrxbadpacket</td><td>Error packets received on the interface</td></tr>
<tr><td>Virtifauthfailure</td><td>Authentication error on the virtual interface</td></tr>
<tr><td>Virtifconfigerror</td><td>Parameter configuration error on the virtual interface</td></tr>
<tr><td>Virtifrxbadpacket</td><td>Error packets received on the virtual interface</td></tr>
</table></td></tr>
<tr><td>isa</td><td>Configures all traps switches related to the LSA. Use this parameter to set the following specified LSA traps switches.
<table>
<tr><td>Lsdbapproachoverflow</td><td>External LSA count has reached the 90% of the upper limit.</td></tr>
<tr><td>Lsdboverflow</td><td>External LSA count has reached the upper limit.</td></tr>
<tr><td>Maxagelsa</td><td>LSA reaching the aging time</td></tr>
<tr><td>Originatelsa</td><td>Generates new LSA</td></tr>
</table></td></tr>
<tr><td>retransmit</td><td>Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches.
<table>
<tr><td>Iftxretransmit</td><td>Packet retransmission on the interface</td></tr>
<tr><td>Virtiftxretransmit</td><td>Packet retransmission on the virtual interface</td></tr>
</table></td></tr>
<tr><td>state-change</td><td>Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches.
<table>
<tr><td>Ifstatechange</td><td>Interface state change</td></tr>
<tr><td>NbrRestartHelper StatusChange</td><td>State change during the neighbor GR process</td></tr>
<tr><td>Nbrstatechange</td><td>Neighbor state change</td></tr>
<tr><td>NssaTranslatorStatusChange</td><td>State change of the NSSA translator</td></tr>
<tr><td>RestartStatusChange</td><td>State change of the GR Restarter on the device</td></tr>
<tr><td>Virtifstatechange</td><td>State change on the virtual interface</td></tr>
<tr><td>VirtNbrRestartHelper StatusChange</td><td>Status change of the virtual neighbor GR process</td></tr>
<tr><td>Virtnbrstatechange</td><td>State change on the virtual neighbor</td></tr>
</table></td></tr>
</table>

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 Examples 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 Description N/A

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

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 Configuring the **lfa** parameter will enable loop-free backup path computation. In this case, the path protection mode for an interface can be specified via the interface mode command.

Configuring the **downstream-paths** parameter will enable downstream path computation.
Configuring the **route-map** parameter can specify backup paths for successfully matched routes via a route map.
It is recommended to use the BFD function with OSPF FRR. In this manner, the device can detect link faults more rapidly to reduce forwarding interruption time. For interface up/down scenarios, to reduce forwarding interruption time of OSPF FRR, you can configure **carrier-delay** *0* for fastest switchover.
Note: OSPF FRR has the following restrictions:
Each route can only generate one backup next hop.
The backup next hop cannot be generated for ECMP.

Configuration Examples 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-nexthop 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 Description N/A

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 [**graceful-period** *grace-period*]
no graceful-restart [**graceful-period**]

Parameter Description

Parameter	Description
grace-period	(optional)Explicitly configures grace-period.
grace-period	User-set GR interval in the range from1 to 1800 seconds. It is the longest time between the OSPF invalidation and the OSPF graceful restart. The default value is 120 seconds.

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.

Configuration Examples The following example enables GR for the OSPF instance 1 and sets the restart interval for GR.

```
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 Description N/A

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	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 determine whether the network changes. If yes, the GR helper will be disabled.
internal-lsa-checking	Checks the change of the LSA of types 1–3 to judge the network whether changes. If so, the GR helper will be disabled.

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 Use this command to enable the GR helper. 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 check the network change by default. The convergence is not performed again until the GR is implemented even if the network changes. Use the **strict-lsa-checking orinternal-lsa-checking** command to enable quick check for the changed network 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 local 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 and modifies the policy of checking network changes.

```
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 Description N/A

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 Description

Parameter	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 Examples The following example configures MD5 authentication for OSPF on fastEthernet 0/1.

```
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 Description N/A

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.
key	Key containing at most eight characters.

Defaults N/A

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*.

```
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 Description N/A

2.27 ip ospf bdf

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 rip 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 **ip ospf bfd** in interface configuration mode command takes precedence over the **bfd all-interfaces** command in routing process configuration mode.
You can use this command to enable the BFD on the specified interface according to the actual

environment. You can also use the bfd all-interfaces command in OSPF process configuration mode to enable BFD on all OSPF interfaces and the **ip rip bfd disable** command to disable BFD on the specified interface.

Configuration Examples N/A

Related Commands

Command	Description
router ospf	Creates the OSPF routing process and enters routing process configuration mode.
bdf all-interfaces	Enables the BFD on all OSPF interfaces.

Platform Description N/A

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
cost	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 Examples The following example configures the OSPF cost of fastEthernet 0/1 to100.

```
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 Description N/A

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 Examples The following example stops sending LSA update packets of fastEthernet 0/1.

```
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 Description N/A

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*

no ip ospf dead-interval

Parameter Description

Parameter	Description
seconds	Defines the interval for determining the neighbor death in seconds. The range is from 0 to 2,147,483,647.

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 You can use the **show ip ospf interface** command to display dead-interval configured for an interface.

Configuration Examples The following example configures the interval for determining the death of the OSPF neighbor on fastEthernet 0/1 to30seconds.

```
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-interval30
```

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 Description N/A

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 Examples The following example prevents the specified interface from generating OSPF packets.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf disable all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.32 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 Examples The following example sets OSPF LFA fast reroute to link and node protection:

```
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 Description N/A

2.33 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 an interface has small superfluous bandwidth or may fail with the master interface at the same time, this interface is not suitable to act as a backup interface. In this case, this command is used.

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

2.34 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
seconds	Interval for sending Hello packets in seconds. The range is from1 to 65535.

Defaults The defaults are as follows:

10secons for Ethernet

10seconsfor PPP or HDLC encapsulated interfaces

10secons for frame relay PTP interfaces

30secons 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 address172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf hello-interval15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the interval for determining the death of the OSPF neighbor.

Platform Description N/A

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
key	Key of up to 16 characters
0	Displays the key in plain text.
7	Displays the key in cipher text.
key-id	Key identifier in the range from1 to 255

Defaults No MD5 key is configured by default.

Command Mode Interface configuration 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-key10md5
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 Description N/A

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 Examples The following example disables the MTU check function on fastEthernet 0/1.

```
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 Description N/A

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 Networks are divided into three types according to the transmission feature of media:

- Broadcast network (Ethernet, token ring and Fiber Distributed-Data Interface (FDDI))
- Non-broadcast network (frame relay and X.25)
- PTP network (High-Level Data Link Control (HDLC), PPP and SLIP)
- The non-broadcast network is further divided into two sub-types by the OSPF operation mode:
- Non-broadcast multi-path access (NBMA) type. NBMA requires all interconnected devices can directly communicate to each other, and only full mesh type connection can meet this requirement. There is no problem in using the Switching Virtual Circuit (SVC)(such as X.25) connections, but it is difficult in case of networking with Permanent Virtual Circuit (PVC) (such as frame relay). The OSPF on the NBMA network operates similarly to that on the broadcast network, where the Designated Device shall be elected to advertise the link state of the NBMA network.
- Point-to-multipoint network type. If the network topology is not a full mesh type non-broadcast network, the OSPF requires the network type to be configured as the point-to-multipoint network type. In the point-to-multipoint network type, OSPF regards all inter-device connections as PTP links and does not participate in the election of the designated device. The point-to-multipoint network type is further divided into the broadcast type and the non-broadcast type. For the non-broadcast type, it is required to manually configure the static neighbor.
- Whatever the default network type of the interface, you must set it to the broadcast network type. For example, the non-broadcast multi-path access network (frame relay and X.25) can be configured as broadcast network, so that the configuration of neighbors can be omitted during the OSPF routing process configuration. The X.25 map and frame-relay map commands may enable the X.25 and frame relay networks with broadcasting capability, so that the OSPF can regard such networks as X.25 and frame relay as broadcast network.
- The interface of the point-to-multipoint network can be configured with one or more neighbors. When the OSPF is configured as the point-to-multipoint network type, multiple host routes may be generated. In contrast to the broadcast network type, the point-to-multipoint network type features the following benefits:
- Easy configuration without need to configure neighbors or election of the designated device
- Small cost, without needing the fully meshed topology

For the dial-up network, frame relay and X.25 network, to manually configure the IP address mapping table, the keyword "broadcast" must be specified to support broadcast.

Configuration Examples The following example configures the frame relay interface network as the broadcast type, which is applicable to the full mesh type frame relay connections.

```
Ruijie(config)# interfaceSerial 1/0
Ruijie(config-if-Serial 1/0)# ipaddress172.16.24.4
255.255.255.0
Ruijie(config-if-Serial 1/0)# encapsulationframe-relay
Ruijie(config-if-Serial 1/0)# ipospfnetworkbroadcast
The following example configures the frame relay interface network as the
```

```
point-to-multipoint type, which is applicable tothe non-full-mesh type frame
relay connections.
Ruijie(config)# interfaceSerial1/0
Ruijie(config-if-Serial 1/0)# ipaddress172.16.24.4
255.255.255.0
Ruijie(config-if-Serial 1/0)# encapsulationframe-relay
Ruijie(config-if-Serial 1/0)# ip ospf network point-to-multipoint
```

The following example configures the frame relay interface network as the broadcast type, with the designated device/backup designated device (DR/BDR) specified, which is applicable to the full or partial mesh type frame relay connections. The following configuration needs to be done on all branch node devices and non-designated devices (limited to become the DR/BDR).

```
Ruijie(config)# interfaceSerial1/0
Ruijie(config-if-Serial 1/0)# ipaddress172.16.24.4
255.255.255.0
Ruijie(config-if-Serial 1/0)# encapsulation frame-relay
Ruijie(config-if-Serial 1/0)# ip ospf network broadcast
Ruijie(config-if-Serial 1/0)# ip ospf priority0
```

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 Description N/A

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
priority	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 Examples The following example configures the priority offastethernet 0/1 as 0.

```
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 Description N/A

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
seconds	Interval for sending the LSU packets in seconds. The range is from 0 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 Description N/A

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 Examples The following example disables the source address check function in the point-to-point link.

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# ip ospf source-check-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.41 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
seconds	LSU packet transmission delay in seconds in the range from 0 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 Examples The following example configures the transmission delay of fastEthernet 0/1 as 10.

```
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 Description N/A

2.42 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 Examples The following example enables the ISPF function.

```
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 Description N/A

2.43 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 Examples The following example logs the neighbor state changes.

```
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 Description N/A

2.44 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
number	Maximum number of DD packets in the range from1 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 Examples The following example sets the maximum number of DD packets to 4.
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 Description N/A

2.45 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).
max-metric-value	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.
seconds	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.

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 Examples The following example configures the LSA maximum metric as 100 seconds after starting the device.

```
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 Description N/A

2.46 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
ip address	IP address of the neighbor
poll-interval *seconds*	(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 *priority*	(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 *cost*	(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 Description N/A

2.47 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
ip-address	IP address of the interface
wildcard	Defines the comparison bits in the IP address, with 0 for exact match and 1 for no comparison
area-id	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 Examples The following example defines:
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 Description N/A

2.48 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
number	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 The following example configures that OSPF instance 10 will be shut down when there are more than

Examples 10 LSAs.

```
Ruijie# config terminal
Ruijie(config)# router ospf 10
Ruijie(config-router)# overflow database 10 hard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.49 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
max-dbsize	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.
wait-time	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 Mode Routing process configuration 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# configterminal
Ruijie(config)# routerospf10
Ruijie(config-router)# overflow database external10 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.50 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 Examples The following example prevents the OSPF from entering the OVERFLOW state when the memory is insufficient.

```
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 Description N/A

2.51 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
interface-type interface-number	Interface to be set as a passive interface
default	Sets all the interfaces as passive interfaces
interface-type interface-number ip-address	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 Description N/A

2.52 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 *[area-tag]*	Redistribution from an IS-IS instance specified in area-tag
ospf *process-id*	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 *metric-value*	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 *route-map-name*	Redistribution filter rule
subnets	Redistributes the routes of non standard networks.
tag *tag-value*	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.

```
Ruijie(config)# router ospf1
Ruijie(config-router)# redistribute ospf 2 subnets
Ruijie(config-router)# redistribute ospf2match
external 1 internal
```

```
Ruijie(config-router)# redistribute isisisis-001
Ruijie(config-router)# redistribute isisisis-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 Description N/A

2.53 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
process-id	ID of an OSPF process. If the process ID is not configured, process 1 is configured.
vrf-name	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 Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.

Configuration Examples The following example creates the OSPF routing process 10 within the specified vrf: vpn_1.

```
Ruijie(config)# router ospf10 vrf: vpn_1
```

Related

Command	Description

Commands

show ip protocols	Displays the routing protocol information.
show ip ospf	Displays the OSPF information.

Platform Description N/A

2.54 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
number	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 Examples The following example sets the maximum number of DD packets to 4.
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	Sets the maximum number of the neighbors that the OSPF routing process can concurrently interact with.

Platform Description N/A

2.55 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
router-id	Router ID in IP address form

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 Examples The following example modifies the router ID to 0.0.0.36.

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# router-id0.0.0.36
```

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.

Platform Description N/A

2.56 show ip ospf

Use this command to display the OSPF information.

show ip ospf [*process-id*]

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the information of the OSPF routing process.

Configuration Examples The following example displays the output of the **show ip ospf** command.

```
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 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 10 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group:240 secs
Number of incomming 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 Adjency 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	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.

this area	
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 Description N/A

2.57 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-mrouters**

Parameter Description

Parameter	Description
process-id	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 Examples The following example displays the output of the **show ip ospf border-mrouters** command.

```
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 Description N/A

2.58 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*] **database** [**adv-router** *ip-address* | { **asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary** } [*link-state-id*] [{ **adv-router** *ip-address* | **self-originate** }] | **database-summary** | **max-age** | **self-originate | detail | brief**]

Parameter Description

Parameter	Description
area-id	(Optional) Displays the area ID.
adv-device	(Optional) Displays the LSA information generated by the specified advertising device.

link-state-id	(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 Examples The following example displays the output of the **show ip ospf database** command.

```
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 Description N/A

2.59 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
process-id	OSPF process ID
interface-type	(Optional) type of the specified interface
interface-number	(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 Examples The following example displays the output of the **show ip ospf interface fastEthernet** *0/1* command:

```
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 Description N/A

2.60 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
process-id	OSPF process ID

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 Examples The following displays the ISPF calculation count in the OSPF area.

```
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 Description N/A

2.61 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
detail	(Optional) Displays the neighbor details.
interface-type	(Optional) Displays the neighbor information of the specified interface

interface-number	
neighbor-id	(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 Examples The following example displays the output of the **show ip ospf neighbor** command.

```
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 Description N/A

2.62 show ip ospf route

Use this command to display the OSPF routes.

show ip ospf [*process-id*] **route** [count]

Parameter Description

Parameter	Description
process-id	OSPF process ID. All OSPF routes will be displayed without an ID specified.
count	Statistics of various OSPF routes

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 Examples The following example displays the output of the **show ip ospf route** command.

```
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 Description N/A

2.63 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
process-id	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 Examples The following example displays the output of the **show ip ospf [***process-id***] spf** command:

```
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 Description N/A

2.64 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
process-id	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 Examples The following example displays the output of the **show ip ospf summary-address** command:

```
Ruijie# show ip ospf summary-address
Summary Address Summary Mask Advertise Status Aggregated subnets
----------- ----------- ------------ ----------- -----------
202.101.0.0     255.255.0.0     advertise       Inactive 0
```

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

2.65 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** *ip-address* | **self-originate**]

Parameter Description

Parameter	Description
process-id	OSPF process ID.
area-id	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 Examples The following example displays the result of the show **ip ospf topology** command:

```
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	Chile 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 Description N/A

2.66 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
process-id	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.
ip-address	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 Examples The following is the output of the **show ip ospf virtual-links** command:

```
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

2.67 summary-address

Use this command to configure the aggregate route out of the OSPF routing domain. Use the **no** form of this command to restore the 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
ip address	IP address of the aggregate route
net-mask	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 *cost*	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 Examples The following example generates an external aggregate route 100.100.0.0/16.

```
Ruijie(config)# router ospf20
Ruijie(config-router)# summary-address100.100.0.0 255.255.0.0
Ruijie(config-router)# redistribute static subnets
Ruijie(config-router)# network200.2.2.0 0.0.0.255 area 1
Ruijie(config-router)# network172.16.24.0 0.0.0.255area 0
Ruijie(config-router)# area1nssa
```

Related Commands

Command	Description
area-range	Configures route convergence on the OSPF area border device.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

2.68 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
arrival-time	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 Examples The following example configures the time delay for the same LSA as 2seconds.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# timers arrival-time 2000
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description N/A

2.69 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 to1800 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 Examples The following example configures the pacing time as 120 seconds.

```
Ruijie(config)# deviceospf 20
Ruijie (config-router)# timers paing lsa-group 120
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description N/A

2.70 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
transmit-time	Configures the interval of sending the LSA grouping. The range is from 10 to 1000.
transmit-count	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: 10

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	Displays the OSPF process information, including the router ID.

Platform Description N/A

2.71 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
spf-delay	Defines the SPF calculation waiting period in seconds. The range is from 0 to 2147483647.After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	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 Description N/A

2.72 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
delay-time	Configures the time delay of generating the LSA first. The range is from 1 to 600000.
hold-time	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is from1 to 600000.
max-wait-time	Configures the maximum interval of successive refreshing the LSA., which determines whether the LSA is refreshed successively. The range is from1 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 Description N/A

2.73 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.
ia-delay	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 ia-delay time runs out.
ase	Calculates the external routes.
ase-delay	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 ase-delay 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 Examples The following example sets the .delay time of the inter-area route calculation to one second.

```
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

2.74 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
spf-delay	Defines the SPF calculation waiting period, in the unit of milliseconds, in the range from1 to 600,000. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations in seconds in the range from1 to 600,000.
spf-max-waittime	Defines the maximum interval between two SPF calculations, in milliseconds in the range from1 to 60,0000.

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.

The value of spf-holdtime cannot be smaller than the value of spf-delay, or the value ofspf-holdtime will be set to be equal to the value of spf-delay;
The value of spf-max-waitime 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
show ip ospf	Displays the configuration information of OSPF
timers spf	Configures the SPF calculation delay. It is recommended to replace the timers spf command with the timers throttle spf command.

Platform Description N/A

2.75 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 Examples

The following example disables the OSPF two-way-maintain function.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# notwo-way-maintain
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the OSPF

Platform Description

N/A

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
area-id	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
spi	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.
key	Specifies an authentication key.

Defaults Authentication is disabled 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 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
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 Description N/A

3.2 area default-cost

Use this command to set the cost of the default route for the ABR in the stub 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
area-id	Area ID of the stub area. It can be an integer or an IPv4 prefix.
cost	Cost of the default route of the stub 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 Description N/A

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 |** [**des** | **3des | aes-cbc [128 | 192 | 256]**] [**0 | 7**] *des-key* **]** [**md5 | sha1**] [**0 | 7**] *key*

no area *area-id* **encryption**

Parameter Description

Parameter	Description
area-id	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.
des	Adopts DES(Data Encryption Standard) encryption.
3des	Adopts 3DES encryption.
aes-cbc[128 | 192 | 256]	Adopts AES-CBC(Advanced Encryption Standard-Cipher Block Chaining) encryption. The key length is 128, 192 or 256 bytes.
des-key	Des encryption key.
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.
Key	Specifies an authentication key.

Defaults Encryption authentication is disabled 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 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-router)# area 1 encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related

Command	Description

Commands

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
area-id	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 *value*	(Optional) Specifies the OSPF default LSA metric. The range is from 0 to 16,777,214, and the default value is 1.
metric-type *type*	(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 *seconds*	(Optional) Configures the stablibity 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 Examples The following example sets the area 1 as an NSSA area.

```
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
area-id	ID of the area in which the addresses are converged.

	It can be an integer or an IPv4 prefix.
ipv6-prefix/prefix-length	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 aggregate 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 Examples The following example converges the routes in area 1.

```
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 Description N/A

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
area-id	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 Mode Routing process configuration 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 LAS 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 Examples The following example enables the ABR in stub area 10 to advertise the default route to the stub area.

```
ipv6 router ospf 1
area 10 stub
area 10 stub no-summary
```

Related Commands

Command	Description
area default-cost	Sets the cost of the default route in the stub area.

Platform Description N/A

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 |** [**des** | **3des |**

aes-cbc [128 | 192 | 256]] [**0 | 7**] *des-key* **]** [**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
area-id	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
Router-id	Neighbor router ID of the virtual link.
hello-interval *seconds*	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 *seconds*	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 *seconds*	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 *seconds*	Delay on the local interface of the virtual link in sending LSA. The range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Specifies the instance corresponding to the virtual link. No virtual link can be established between different instances. Range: 0.-255
authentication ipsec spi *spi* [**md5	sha1**] [**0	7**] *key*	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. *spi* 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. *key* specifies an authentication key.
encryption ipsec spi *spi* **esp [null |** [**des**	**3des	aes-cbc [128	192	256]**] [**0	7**] *des-key*	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. *spi* specifies a security parameter index, in the range from 256 to 4294967295. **null** specifies the null encryption mode. des specifies DES(Data Encryption Standard) encryption. 3des specifies 3DES encryption. aes-cbc 128 specifies 128-byte aes-cbc encryption.

	aes-cbc 192 specifies 192-byte aes-cbc encryption. aes-cbc 256 specifies 256-byte aes-cbc encryption. des-key specifies the DES encryption key. **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. *key* 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 disabled 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 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 Examples The following example configures a virtual link.

```
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 Description N/A

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 *ref-bw*	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 Examples N/A

Related Commands

Command	Description
ipv6 router ospf *process-id*	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 Description N/A

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
process-id	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 Examples The following example restarts the OSPF process.

```
enble
clear ipv6 ospf process
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 *metric*	(Optional) Initial metric value of the default route, in the range from 0 to 16777214
metric-type *type*	(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 *map-name*	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.

The routers in the stub area cannot generate external default routes.

Configuration Examples The following example generates a default route.

```
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 Description N/A

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
metric-value	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 Examples The following example sets the default metric for the routes to be redistributed to 10.

```
default-metric 10
```

Related Commands

Command	Description
redistribute	Redistributes the routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

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
distance	Sets the management distance of the route, in the range from 1 to 255.
intra-area *distance*	Sets the management distance of the intra-area route, in the range from1 to 255.
inter-area *distance*	Sets the management distance of the inter-area route, in the range from 1 to 255.
external *distance*	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 Examples the following example sets the OSPFv3 external route management distance to 160.

```
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 Description N/A

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
name	Specifies an ACL filtering rule.
prefix-list *prefix-list-name*	Specifies a prefix list filtering rule.
interface-type interface-number	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 Examples 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 Description N/A

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
name	Specifies the ACL filtering rule.
prefix-list *prefix-list-name*	Specifies the prefix list filtering rule.
**bgp	connected	isis** [*area-tag*]	**ospf** process-id	**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 Examples 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 Description N/A

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 OSFPv3 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 Examples The following example enables users to operate the OSPFv3 process with the process number of 100 through SNMP.

```
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 Description N/A

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 | VirtIfStateChange | VirtNbrStateChange**]]

no enable traps [**error** [**IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket**] | **state-change** [**IfStateChange | NbrStateChange | 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; **VirtIfStateChange** specifies state change of a virtual interface; **VirtNbrStateChange** specifies state change of a virtual neighbor.
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.
key	Specifies an authentication key.

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 Examples The following example enables all traps of OSPFv3 process 100.

```
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 Description N/A

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 disable this function or restore the GR period setting..
graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]
no graceful-restart [*graceful-period*]

Parameter Description

Parameter	Description
grace-period *grace-period*	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 1,800 in the unit of seconds. The default is 120 seconds.
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.

Configuration Examples 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 Description N/A

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 restore the default setting.
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 from assisting 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 orinternal-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 Description N/A

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
process-id	OSPF process ID.
area *area-id*	OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix.
instance *instance-id*	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 interface 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 Description N/A

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*] [**instance** *instance-id*]

no ipv6 ospf authentication

Parameter Description

Parameter	Description
null	Indicates that authentication is not performed.
spi	Specifies a security parameter index, in the range from 256 to 4,294,967,295.
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.
key	Specifies an authentication key.
instance *instance-id*	Specifies the OSPFv3 instance ID on the interface, in the range from 0 to 255.

Defaults Authentication is not configured 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 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
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 N/A

Description

3.22 ipv6 ospf bdf

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 [**dsable**] [**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 *instance-id*	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 enanble 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 Examples N/A

Related Commands

Command	Description
ipv6 router ospf *process-id*	Starts the OSPFv3 routing process and enter into the routing process configuration mode.
bdf all-interfaces	Enables the BFD on all OSPFv3 interfaces.

Platform Description N/A

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
Cost	Cost of interface, in the range from 0 to 65535.
instance *instance-id*	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 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.

The default costs of OSPFv3 interfaces for several typical lines are:

- 64K serial line: 1562;
- E1 line: 48
- 10M Ethernet: 10
- 100M Ethernet: 1

The OSPFv3 cost configured with the command **ipv6 ospf cost** will overwrite the default configuration.

Configuration Examples The following example sets the cost of the interface to 1:

```
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 Description N/A

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* [**instance** *instance-id*]

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	Dead interval of neighbors. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

The dead interval of neighbors is four times longer than the hello interval.

Command Mode

Interface configuration mode

Usage Guide

The dead interval of neighbors must be longer than the hello interval. You can use the **show ipv6 ospf interface** command to display the dead interval of neighbors 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 |** [**des** | **3des | aes-cbc [128 | 192 | 256]**] [**0 | 7**] *des-key* **]** [**md5 | sha1**] [**0 | 7**] *key*] [**instance** *instance-id*]

no ipv6 ospf encryption [**instance** *instance-id*]

Parameter Description

Parameter	Description

null	Indicates that encryption authentication is not performed.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.
des	Adopts DES(Data Encryption Standard) encryption.
3des	Adopts 3DES encryption.
aes-cbc[128 | 192 | 256]	Adopts AES-CBC(Advanced Encryption Standard-Cipher Block Chaining) encryption. The key length is 128, 192 or 256 bytes.
des-key	Des encryption key.
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.
key	Specifies an authentication key.
instance *instance-id*	Specifies the OSPFv3 instance ID on the interface, in the range from 0 to 255.

Defaults Encryption authentication is disabled 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 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
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 Description N/A

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
seconds	Interval for sending the Hello message. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	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.

Configuration Examples The following example sets the interval for the interface to send the Hello message to 20 seconds.

```
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 Description N/A

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 *instance-id*	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 Examples The following example disables the MTU check function on the ethernet 1/0.

```
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 Description N/A

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 *cost*	(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 *seconds*	(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 *priority*	(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 *instance-id*	(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 Examples The following example shows how to configure the OSPFv3 neighbor as follows: IPv6 address: 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 Description N/A

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 Description

Parameter	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
number-value	The priority of the interface. Its range is from 0 to 255.

instance *instance-id*	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 *instance-id*	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
seconds	Interval for retransmitting the LSA. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface.

Defaults The default is five seconds.

Command Interface configuration mode.

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 Examples The following example sets the interval for retransmitting the LSA to 10 seconds.

```
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 Description N/A

3.32 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
seconds	The delay in sending LSA. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	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

Command	Description

Commands		
	show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description N/A

3.33 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
process-id	OSPFv3 process ID number. Without the process number configured, it indicates that process 1 is started.
vrf-name	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 Examples The following example starts OSPFv3 process in the specified VRF VPN1.

```
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 Description N/A

3.34 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 Description

Parameter	Description
number	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

3.35 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 Examples 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 Description N/A

3.36 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
number	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 Description N/A

3.37 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.
interface-type interface-number	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 Description N/A

3.38 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**] } | **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**]} | **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*[area-tag]*	The isis is redistributed. The area-tag specifies a particular isis instance.
ospf *process-id*	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. All sub-type OSPFv3 routes are redistributed by default.
metric *metric-value*	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 *map-map-name*	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 *tag-value*	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 Examples The following example redistributes the direct route and associates route-map test :

```
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
default-information originate	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 Description N/A

3.39 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
router-id	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 Description N/A

3.40 summary-prefix

Use this command to configure the aggregate 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** *number* | **cost** *cost*]

no summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise |** [**tag**] [**cost**]]

Parameter Description

Parameter	Description
ipv6-prefix/*prefix-length*	Address range of the aggregate route
not-advertise	Does not advertise the aggregate route to neighbors. Absence of this parameter means to advertise.
tag *number*	Tag value redistributed to the OSPFv3 inner route, in the range from 0 to 4,294,967,295.
cost *cost*	Cost value of the aggregate route, in the range from 0 to16,777,214.

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 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 aggregate 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.

The **summary-prefix** command is valid only on the ASBR now, and causes the convergence for only

redistributed routes.

Configuration Examples The following example configures the external route within the 2001:DB8::/64 to the aggregate route 2001:DB8::/64 to advertise it.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# 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

3.41 show ipv6 ospf

Use this command to display the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter Description

Parameter	Description
process- id	OSPF process ID number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about the OSPFv3 process.

```
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 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
LSA interval 5 secs, Minimum LSA arrival 1000 msecs
```

```
Pacing lsa-group: 30 secs
Number of incomming 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 Adjency 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
```

With the BFD for OSPFv3 configured, the content of “BFD is enabled” is added to the original information displayed. For example:

```
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 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
LSA interval 5 secs, Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming 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 Adjency Changes : Enabled
Number of areas in this router is 2
BFD is enabled
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
```

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.
router-id	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 Description N/A

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
process- id	OSPF process ID number
lsa-type	The LSA types are as follows: 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 *router-id*	Displays the LSA information generated by the specified router.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the information about the OSPFv3 process database.

```
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 Description N/A

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 Description

Parameter	Description
interface-type interface-number	Specifies the interface type and interface number.
process- id	OSPFv3 process ID
brief	Displays the interface summary.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the information about the OSPFv3 interface.

```
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
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the

	OSPFv3 process.

Platform Description N/A

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** |**statistics**]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number
detail	Displays details about the neighbor.
interface-type interface-number	Interface type and interface number
neighbor-id	Neighbor's router ID
statistics	Statistics about the neighbor.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following command displays the brief information about the OSPFv3 neighbor.

```
Ruijie# show ipv6 ospf neighbor
OSPFv3 Process (1), Neighbores, 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
```

The following command displays the details of OSPFv3 neighbors:

```
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
```

If the BFD has been enabled for the forwarding path of the neighbor , the content of “BFD session state up” is added to the information displayed. For example:

```
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 Description N/A

3.45 show ipv6 ospf route

Use this command to display the OSPFv3 route information.

show ipv6 ospf [*process- id*] **route** [**count**]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number.
count	Total number of OSPFv3 routes

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about OSPFv3 routes.

```
Ruijie# show ipv6 ospf route
```

```
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area, E1 - OSPF
external type 1, E2 - OSPF external type 2
Destination                              Metric
Next-hop
E2 2222::/64                                  1/20
via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O  3333::/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 Description N/A

3.46 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
process- id	OSPFv3 process ID number

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the external route convergence information of OSPFv3.

```
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 Description N/A

3.47 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
process- id	OSPFv3 process ID number
area-id	Area ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following command displays the topology information about each area of OSPFv3.

```
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   --
```

1

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

3.48 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
process- id	OSPFv3 process ID number

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following command displays the information about the OSPFv3 virtual link.

```
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

3.49 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

Parameter	Description
arrival-time	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.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers lsa arrival 2000
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information, including identifiers of routing devices.

Platform Description N/A

3.50 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

Parameter	Description
seconds	Specifies the LSA group pace 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 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 Examples The following example sets the LSA group pace interval to 120 seconds.

```
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 Description N/A

3.51 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
transmit-time	Specifies the interval for sending LSA groups. The range is from 10 to 1000 in the unit of milliseconds.
transmit-count	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 **transimit-time** and **transimit-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 **transimit-time** value and increase the **transimit-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 Description N/A

3.52 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
spf-delay	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.
spf-holdtime	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 Description N/A

3.53 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
delay-time	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.
hold-time	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
max-wait-time	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 Mode Routing process configuration 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
show ipv6 ospf	Displays OSPFv3 process information.

Platform Description N/A

3.54 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.
ia-delay	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 ia-delay time runs out.
ase	Calculates the external routes.
ase-delay	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 ase-delay time runs out.

Defaults The default *ia-delay* is 0 and *ase-delay* is 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 Examples The following example sets the .delay time of the inter-area route calculation to one second.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.55 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
spf-delay	Specifies an SPF calculation delay after the topology change information is received. The range is from 1 to 600,000 in the unit of milliseconds.
spf-holdtime	Specifies a shortest interval between two SPF calculations. The range is from 1 to 600,000 in the unit of milliseconds.
spf-max-waittime	Specifies a longest interval between two SPF calculations. The range is from 1 to 600,000 in the unit of milliseconds.

Defaults The default *spf-delay* is 1,000. *spf-holdtime* is 5,000 and *spf-max-waittime* is 10,000.

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.

- The spf-holdtime cannot be smaller than spf-delay, or the spf-holdtime will be set to be equal to spf-delay;
- The spf-max-waitime cannot be smaller than spf-holdtime, or the spf-max-waittime will be set to be equal to spf-holdtime automatically;
- The configuration of the timers spf command and of the timers throttle spf command are overwritten each other.
- 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 Description

N/A

3.56 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 Description

Parameter	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 Examples The following example disables two-way OSPFv3 maintenance.

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# no two-way-maintain
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.

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
unicast	Optional, use the 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	Exit 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. The **no** form of this command is used 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. The **no** form of this command is used to cancel the password set.

area-password *password-string* [**send-only**]

no area-password [**send-only**]

Parameter Description

Parameter	Description
password-string	Character string of the plaintext authentication password with the longest length being 254 characters..
send-only	Specify the plaintext authentication password of Level-1 area applicable to the packets sent only, but not to the packets received.

Defaults By default, no authentication password is set.

Command Mode IS-IS routing process configuration mode

Usage Guide IS-IS routing process configuration mode

Configure this command to perform the authentication on the LSP, CSPN and PSNP packets received in the Level-1 domain and send the packets taking with the authentication information. In the same area, all IS-IS devices must be configured the same password.

If the **authentication mode** command has been executed, this command will not be configured successfully. You need to delete the **authentication mode** command first.
Running the **no area-password send-only** command can only disable the **send-only** option.

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	Set the Level-2 domain password.
authentication mode	Specify 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** | l**evel-2**]

Parameter Description

Parameter	Description
name-of-chain	Key-chain name with the maximum length being 255.
level-1	Specify the authentication key-chain of the Level-1.
level-2	Specify the authentication key-chain of the Level-2.

Defaults By default, the authentication key-chain is not specified.

Command Mode N/A

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 254 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 Examples The following example specifies the authentication in the IS-IS area using the key-chain named *kc*:

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication key-chain kc level-1
```

Related Commands

Command	Description
authentication mode	Specify the IS-IS authentication mode.
authentication send-only	Specify the IS-IS authentication applicable to the sent packets only, but not to packets received.
key-chain	Configure the key-chain.

Platform Description N/A

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	Specify the MD5 authentication mode to use.
text	Specify the plain-text authentication mode to use.
level-1	Specify the authentication mode taking effect on the Level-1.
level-2	Specify the authentication mode taking effect on the Level-2.

Defaults By default, the authentication mode is not specified.

Command Mode IS-IS routing process configuration 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 Examples The following example specifies authentication in the IS-IS area to be the MD5 authentication mode.

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication mode md5 level-1
```

Related Commands

Command	Description
area-password	Set the area plaintext authentication password.
authentication key-chain	Specify the key-chain used by the IS-IS authenction.
authentication send-only	Specify the IS-IS authentication applicable to the packets sent only, but not to the packets received.
domain-password	Set the domain plaintext authentication password.

Platform Description N/A

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. The **no** form of this command cancels this mode, that is, restore 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	Specify setting **send-only** on the Level-1.
level-2	Specify 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 recieved.

Command Mode IS-IS routing process configuration 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 Examples The following example specifies the authentication in the IS-IS area to be the **send-only** mode.

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication send-only level-1
```

Related Commands

Command	Description
authentication key-chain	Specify the IS-IS authentication key-chain.
authentication mode	Specify the mode of IS-IS authentication.
key-chain	Configure the key-chain.

Platform Description N/A

4.7 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 By default, no IS-IS neighbor relation table is cleared.

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 Examples

```
Ruijie# clear clns neighbors
```

Related Commands

Command	Description
clear isis	Clear all IS-IS data structure.

Platform Description N/A

4.8 clear isis *

Use this command to clear the data structure of all IS-ISs.

clear isis *

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the IS-IS data structure is not cleared.

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	Clear all IS-IS neighbors.

Platform Description N/A

4.9 clear isis counter

Use this command to clear various statistics of IS-IS.

clear isis [*tag*] **counter**

Parameter Description

Parameter	Description
tag	IS-IS instance

Defaults By default, various statistics of IS-IS are not cleared.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# clear isis counter
```

Related Commands

Command	Description
clear isis *	Clear the data structure of all IS-ISs.

Platform Description N/A

4.10 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 Description

Parameter	Description
map-name	(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 Mode IS-IS routing process configuration mode or address-family ipv6 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 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 Description N/A

4.11 distance

Use this command to set the management distance of the IS-IS routes. Use the **no** form of this command to restore the management distance to the default value.

distance *my-cost*

no distance

Parameter Description

Parameter	Description
my-cost	Distance value in the range of 1 to 255.

Defaults By default, the distance is 115.

Command Mode IS-IS routing process 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 Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# distance 100
```

Related Commands

Command	Description
isis metric	Set the metric value of the interface.

Platform Description N/A

4.12 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 *password-string* [**send-only**]
no domain-password [**send-only**]

Parameter Description

Parameter	Description
password-string	Character string of the plain-text authentication password with the longest length being 254 characters.
send-only	Specify the plain-text authentication password of the Level-2 domain applicable to the packets sent only, but not to the packets received.

Defaults By default, no authentication password is set.

Command Mode IS-IS routing process configuration mode

Usage Guide Configure this command to perform the authentication on the LSP, CSPN and PSNP packets received in the Level-2 domain and send the packets taking with the authentication information. In the Level-2 domain, all IS-IS devices must be configured the same password.
If the **authentication mode** command has been executed, this command will not be configured successfully. You need to delete the **authentication mode** command first.
Running the **no area-password send-only** command can only disable the **send-only** option

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# domain-password redgiant
```

Related Commands

Command	Description
area-password	Set the plain-text authentication password of Level-1 area.
authentication mode	Specify the IS-IS authentication mode.

Platform Description N/A

4.13 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 Mode IS-IS routing process configuration 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 Examples The following example binds the MIB with an IS-IS process.

```
Ruijie(config)# router isis
Ruijie(config-router)# enable mib-binding
```

Related Commands

Command	Description
graceful-restart helper disable	Disable the IS-IS GR Help capability.
isis hello-interval	Set the interval of sending Hello packets.
isis hello-multiplier	Set the Hello holdtime multiplier for the IS-IS interface.

Platform Description N/A

4.14 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.
traps set	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	Disable the IS-IS GR Help capability.
isis hello-interval	Set the interval of sending Hello packets.
isis hello-multiplier	Set the Hello holdtime multiplier for the IS-IS interface.

Platform Description N/A

4.15 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 Examples The following example exit IS-IS address family IPv6 configuration mode.

```
Ruijie (config-router-af)#exit-address-family
Ruijie (config-router)#
```

Related Commands

Command	Description
graceful-restart helper disable	Disable the IS-IS GR Help capability.

isis hello-interval	Set the interval of sending Hello packets.
isis hello-multiplier	Set the Hello holdtime multiplier for the IS-IS interface.

Platform Description N/A

4.16 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 With this command used, after the device restart, the IS-IS protocol state is allow to restore to the state before restart without influencing the data forwarding in the condition of network state unchanged.

With the IS-IS GR Restart capability enabled on the device of multiple management boards, the hold time for maintaining the IS-IS adjacent relation shall not be less than 40 seconds to ensure the success of IS-IS graceful restart when the management boards are switched over suddenly. You can configure the hold time using the **isis hello-interval** and **isis hello-multiplier** commands. When the holdtime is less than 40s, the holdtime in the Hello packet header is set to 40 seconds by default.

Note: The IS-IS device needs the help of the GR Helper neighbor device to implement the graceful-restart.

Configuration Examples The following example enables the IS-IS GR Restart capability.

```
Ruijie(config)# router isis
Ruijie(config-router)# graceful-restart
```

Related Commands

Command	Description
graceful-restart helper disable	Disable the IS-IS GR Help capability.
isis hello-interval	Set the interval of sending Hello packets.
isis hello-multiplier	Set the Hello holdtime multiplier for the IS-IS interface.

Platform Description N/A

4.17 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 this interval to the default value.

graceful-restart grace-period *seconds*

no graceful-restart grace-period

Parameter Description

Parameter	Description
second	Time interval allowed for the device graceful-restart, in the range of 1 to 65,535 seconds.

Defaults The default value is 300 seconds.

Command Mode IS-IS routing process configuration mode

Usage Guide N/A

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	Enable the IS-IS GR Restart capability.
show isis graceful-restart	Show the status information of the IS-IS GR Restart.

Platform Description N/A

4.18 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	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 Examples The following example disables the IS-IS GR Helper capability.

```
Ruijie(config)# router isis
Ruijie(config-router)# graceful-restart helper disable
```

Related Commands

Command	Description
graceful-restart	Enable the IS-IS GR Restart capability.

Platform Description N/A

4.19 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

4.20 ignore-lsp-errors

Execute this command to ignore the LSP checksum errors. The **no** form of this command does 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 Mode IS-IS routing process configuration 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 executes 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 Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# ignore-lsp-errors
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.21 ip router isis

Use this command to enable the IPv4 IS-IS 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. The **no** form of this command disables the IPv4 IS-IS routing on the specified interface.

ip router isis [*tag*]

no ip router isis [*tag*]

Parameter Description

Parameter	Description
tag	IS-IS instance name.

Defaults By default, the Ipv4 IS-IS is disabled on the interface.

Command Mode Interface configuration 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 Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip router isis
```

Related Commands

Command	Description
ipv6 router isis	Enable the IPv6 IS-IS on the interface.
router isis	Create IS-IS instances.

Platform Description N/A

4.22 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. The **no** form of this command disables the IPv6 IS-IS routing on the specified interface.

ipv6 router isis [*tag*]
no ipv6 router isis [*tag*]

Parameter Description

Parameter	Description
tag	IS-IS instance name

Defaults By default, the Ipv6 IS-IS routiong 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	Enable the IPv4IS-IS on the interface.
router isis	Create IS-IS instances.

Platform Description N/A

4.23 isis authentication key-chain

Use this command to set the key-chain used by the IS-IS interface authentication. The **no** form of this command cancels 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
name-of-chain	Key-chain name with the maximum length being 255.
level-1	Specify the authentication key-chain of the Level-1.
level-2	Specify 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 254 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	Specify the mode of IS-IS interface authentication.
isis authentication send-only	Specify the IS-IS interface authentication only applicable to the packets sent, but not to the packets received.
key-chain	Configure the key-chain.

Platform Description N/A

4.24 isis authentication mode

Use this command to specify the mode of IS-IS interface authentication. The **no** form of this command cancels the specified IS-IS interface authentication mode.
isis authentication mode { **md5** | **text** } [**level-1** | **level-2**]

no isis authentication mode { **md5** | **text** } [**level-1** | **level-2**]

Parameter Description

Parameter	Description
md5	Specify the MD5 authentication mode.
text	Specify the plain-text authentication mode.
level-1	Specify the interface authentication mode to take effect on the Level-1.
level-2	Specify 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	Specify the key-chain used by the IS-IS interface authentication.
isis authentication send-only	Specify the IS-IS interface authentication to only apply on the packets sent, but not on the packets received.
key-chain	Configure the key-chain.
isis password	Set the plain-text authentication password for the packets transmit on the IS-IS interface.

Platform Description N/A

4.25 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. The **no** form of this command cancels this authentication mode, that is, 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	Specify the key-chain used by the IS-IS interface authentication.

isis authentication mode	Specify the mode of the IS-IS interface authentication.
key-chain	Configure the key-chain.

Platform Description N/A

4.26 isis circuit-type

Use this command to set the circuit-type for the IS-IS interface. The **no** form of this command restores the circuit-type to the default setting.

isis circuit-type { **level-1** | **level-1-2** | **level-2-only** }

no isis circuit-type

Parameter Description

Parameter	Description
level-1	Form the Level-1 adjacency.
leve-2-only	Form the Level-2 adjacency.
level-1-2	Form the Level-1-2 adjacency.

Defaults By default, the circuit-type is Level-1-2.

Command Mode Interface configuration mode

Usage Guide If the circuit-type of Level-1 or Level-2-only is configured, then IS-IS will only send PDUs of the same level.

If is-type is configured to Level-1 or Level-2-only, the IS-IS instance will only process data at this level, that is, this Interface will only send the Level PDUs with is-type being same as circuit-type.

Configuration Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis circuit-type level-2-only
```

Related Commands

Command	Description
isis-type	Set the Level of IS-IS instance.

Platform Description N/A

4.27 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. The **no** form of this command restores this interval to the default value.

isis csnp-interval *interval* [**level-1** | **level-2**]

no isis csnp-interval [*interval*] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
interval	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 Description N/A

4.28 isis hello-interval

Use this command to set the interval for sending Hello packets on the interface, with the unit being second. The **no** form of this command restores the interval to the default value.

isis hello-interval { *interval* | **minimal** } [**level-1** | **level-2**]

no isis hello-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description
interval	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

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis hello-interval 5 level-1
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if)# isis hello-interval minimal
```

Related Commands

Command	Description
isis hello-multiplier	Set the multiplier of the Hello hold timer.

Platform Description N/A

4.29 isis hello-multiplier

Use this command to set the multiplier of Hello hold timer. The **no** form of this command restores the value to the default.

isis hello-multiplier *multiplier-number* [**level-1 | level-2**]

no isis hello-multiplier [*multiplier-number*] [**level-1 | level-2**]

Parameter Description

Parameter	Description
multiplier-number	Multiplier value in the range of 2 to 100.

Defaults By default, the multiplier is 3..

Command Mode IS-IS routing process 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 Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# isis hello-multiplier 5
```

Related Commands

Command	Description
isis hello-interval	Set the interval for sending the Hello packets.

Platform Description N/A

4.30 isis hello padding

Use this command to specify the filling mode for the IS-IS Hello packets. The **no** form of this command does not fill the 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 Interface configuration mode

Mode

Usage Guide Fill the IS-IS Hello packets to advertise the MTU supported to the neighbors.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# no isis hello padding
```

Related Commands

Command	Description
isis hello-interval	Set the interval for sending the Hello packets.

Platform Description N/A

4.31 isis lsp-interval

Use this command to set the interval for the LSP PDU transmission. The **no** form of this command restores the interval to the default value.

isis lsp-interval *interva*l

no isis lsp-interval

Parameter Description

Parameter	Description
interval	Interval time in the range of 1 to 4294967295, with the unit being millisecond.

Defaults By default, the lsp-interval is 33ms.

Command Mode Interface configuration mode

Usage Guide This command is used to set the minimal interval for sending the LSPs on the interface, with the unit being millisecond.

Configuration Examples

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis lsp-interval 100
```

Related Commands

Command	Description
isis retransmit-interval	Set the LSP retransmission interval in the P2P network.

Platform Description N/A

4.32 isis mesh-group

Use this command to add the interface to the specified mesh-group. The **no** form of this command is used to separate the interface from the mesh-group.

isis mesh-group { **blocked** | *mesh-group-id* }

no isis mesh-group

Parameter Description

Parameter	Description
blocked	Block all LSP forwarding on the interface.
mesh-group-id	Add the interface to the mesh-group of specified mesh-group-id with the range being 1 to 4294967295.

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 subintefaces, 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 Examples

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)#isis mesh-group 1
```

Related Commands

Command	Description
isis network point-to-point	Set the Broadcast interface type of IS-IS to Point-to-Point.

Platform N/A

Description

4.33 isis metric

Use this command to set the metric for the interface. The **no** form of this command restores the metric to the default value.

isis metric *metric* [**level-1** | **level-2]**

no isis metric [*metric*] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
metric	Metric value in the range of 1 to 63.
level-1	Set this metric to apply on the Level-1 circuit.
level-2	Set 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 Examples

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)#isis metric 1
```

Related Commands

Command	Description
metic-style	Set the metric type.
isis wide-metric	Set the wide metric of the IS-IS interface.

Platform Description N/A

4.34 isis network point-to-point

Use this command to set the IS-IS Broadcast interface to the Point-to-Point type. The **no** form of this command restores the interface type to the Broadcast.

isis network point-to-point

no isis network point-to-point

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the **isis network point-point** is not executed.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis network point-to-point
```

Related Commands

Command	Description
isis mesh-group	Add the IS-IS interface into the specified mesh group.

Platform Description N/A

4.35 isis password

Use this command to set the plain-text authentication password for the Hello packet transmitted on the interface. The **no** form of this command cancels the password settings.

isis password *password-string* [**send-only**] [**level-1** | **level-2**]

no isis password [**send-only**] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
password-string	The character strings of the plain-text authentication password with the longest length being 254 characters.
send-only	The plain-text authentication password is only applicable to the packets sent. No authentication will be performed on the packets received.
level-1	This password applies to the Level-1 circuit.
level-2	This password applies to the Level-2 circuit.

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 Examples

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis password redgiant
```

Related Commands

Command	Description
isis authentication mode	Specify the mode of the IS-IS interface authentication.

Platform Description N/A

4.36 isis priority

Use this command to set the priority for the DIS election on the LAN. The **no** form of this command restores the priority to the default value.
isis priority *value* [**level-1** | **level-2**]
no isis priority [*value*] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
value	Value of the priority in the range of 0 to 127.
level-1	This priority is applied on the Level-1 circuit.
level-2	This priority is applied on the Level-2 circuit.

Defaults The default priority value is 4 and it is applied on both Level-1 and Leve-2 circuit.

Command Mode Interface configuration 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 Examples

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis priority 127 level-1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.37 isis retansmit-interval

Use this command to set the LSP retransmission interval. The **no** form of this command restores the interval to the default value.

isis retransmit-interval *interval-time*

no isis retransmit-interval

Parameter Description

Parameter	Description
interval-time	Interval time in the range of 0 to 65535 with the unit being second.

Defaults 5s

Command Mode Interface configuration mode

Usage Guide This command is used to set the LSP retransmission interval. The retransmission refers to that on a point-to-point link, if the local router fails to receive the PSNP reply after sending LSPs in the retransmit-interval, it will retransmit that LSP packets.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface serial 0/1
Ruijie(config-if)# isis retransmit-interval 10
```

Related Commands

Command	Description
isis lsp-interval	LSP publishing interval on the interface.

Platform Description N/A

4.38 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 neigbor 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 Examples 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	Set the Metric type.
isis metric	Set the Metric value of the interface.

Platform Description N/A

4.39 isis wide-metric

Use this command to set the wide metric of the interface. The **no** form of this command is used to restore the wide metric to the default value.

isis wide-metric *metric* [**level-1** | **level-2**]

no isis wide-metric [*metric*] [**level-1** | **level-2**]

Parameter Description

Parameter	Description
metric	Metric value in the range of 1 to 16777241.
level-1	Set this Metric to apply on the Level-1 circuit.
level-2	Set 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 Examples

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)#isis wide-metric 1000
```

Related Commands

Command	Description
metric-type	Set the Metric type.
isis metric	Set the Metric value of the interface.

Platform Description N/A

4.40 is-type

Use this command to specify the level for the IS-IS process. The **no** form of this command is used 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	Specify the IS-IS process running on the Level-1 only.
level-1-2	Specify the IS-IS process running on both Level-1 and Level-2.
level-2-only	Specify 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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# is-type level-1
```

Related Commands

Command	Description
isis circuit-type	Set the type of Interface circuit.

Platform Description N/A

4.41 log-adjacency-changes

Use this command to log the changes of the IS adjacency status in case of debug disabled. The **no** form of this command disables this function.

log- adjacency-changes

no log- adjacency-changes

Parameter Description

Parameter	Description
N/A	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 Examples

```
Ruijie(config-router)# log-adjacency-changes
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

4.42 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	Enable the LSP fragment extension mode for the Level-1 only.
level-2	Enable 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

4.43 lsp-gen-interval

Use this command to set the minimal interval of the LSP generation. The **no** form of this command restores it to the default value.

lsp-gen-interval [**level-1** | **level-2**] *value*

no lsp-gen-interval

Parameter Description

Parameter	Description
value	In the range of 1 to 20 with unit being second.
level-1	The minimal interval is applicable on the Level-1 IS-IS.
level-2	The minimal interval is applicable on the Level-2 IS-IS.

Defaults By default, this command is not configured and the interval of the minimal generation is 5s, it is effective on both Level-1 an Level-2

Command Mode IS-IS routing process configuration mode

Usage Guide The LSP generation interval refers to the interval of the generation time between the new version LSP and old LSP. The smaller this value, the faster the network convergence is, but it also causes the frequent network flood. This value must be set properly according to different environments

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# lsp-gen-interval 5
```

Related Commands

Command	Description
lsp-refresh-interval	LSP refresh interval.

Platform Description N/A

4.44 lsp-refresh-interval

Use this command to set the LSP refresh interval. The **no** form of this command restores it to the default value.

lsp-refresh-interval *interval*

no lsp-refresh-interval

Parameter Description

Parameter	Description

interval	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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# lsp-refresh-interval 600
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.45 max-area-addresses

Use this command to set the maximal number of area address allowed. The **no** form of this command restores it to the default value.
max-area-addresses *value*
no max-area-addresses

Parameter Description

Parameter	Description
value	The maximal number of area address allowed, in the range of 3 to 6.

Defaults By default, the max-area-addreses 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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# max-area-addresses 5
```

Related Commands

Command	Description
net	Set the IS-IS NET(Network Entry Title) address.

Platform Description N/A

4.46 max-lsp-lifetime

Use this command to set the maximum value of the LSP lifetime. The **no** form of this command restores it to the default value.

max-lsp-lifetime *value*

no max-lsp-lifetime

Parameter Description

Parameter	Description
value	Maximum value of the LSP lifetime in the range of 1 to 65535, 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# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# max-lsp-lifetime 1500
```

Related Commands

Command	Description
lsp-refresh-interval	LSP refresh interval.

Platform Description N/A

4.47 metric-style

Use this command to set the metric style. The **no** form of this command restores the metric style to the default value.

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	Use the old metric style with the router interface metric ranging from 1 to 63.
wide	Use the new metric style with the router interface metric ranging from 1 to 16777214
transition	Allow 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 Mode IS-IS routing process configuration 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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# metric-style wide
```

Related Commands

Command	Description
isis metric	Set the metric of the interface.
isis wide-metric	Set the wide metric of the interface.

Platform Description N/A

4.48 net

Use this command to set the IS-IS NET (Network Entry Title) address. The **no** form of this command deletes this NET address.
net *net-address*
no net *net-address*

Parameter Description

Parameter	Description
net-address	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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# net 49.0000.0001.0002.0003.00
```

Related Commands

Command	Description
router isis	Create IS-IS instances.

Platform Description N/A

4.49 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	Configure the MT transition mode.

Defaults By default, multitopology is not configured, namely, IS-IS does not support IPv6 unicast topology.

Command Mode IS-IS address-family IPv6 configuration mode

Usage Guide When this command is not configured, IPv4 and IPv6 share the same IS-IS physical topology, which is also called default topology.

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.

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 apply 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 Examples The following example enables IS-IS to support IPv6 unicast topology.

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# address-family ipv6
Ruijie(config-router-af)# multi-topology
```

Related Commands

Command	Description
router isis	Create IS-IS instances.

Platform Description N/A

4.50 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	Configure IS-IS disabled interfaces as passive.
interface-type	Indicates the interface type.
interface-number	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 Examples The following example configures interface GigabitEthernet 0/0 as passive.

```
Ruijie(config)# router isis 1
Ruijie(config-router)# passive-interface GigabitEthernet 0/0
```

Related Commands

Command	Description
router isis	Create IS-IS instances.

Platform Description N/A

4.51 redistribute

Use this command to redistribute the routes from one routing protocol into another routing protocol. The **no** form of this command deletes 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
process-id	OSPF process ID, in the range of 1 to 65535.
match { **internal**	**external** [**1**	**2**]	**nssa-external** [**1**	**2**] }	Redistribute 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 *metric-value*	Set 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** }	Set 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 *map-tag*	Set 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 *map-tag* shall not be over 32 characters. No route-map is configured by default.
level-1 | **level-1-2** | **level-2**	Specify 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 Mode IS-IS routing process configuration mode , IS-IS address-family ipv6 mode

Usage Guide Configure "**no redistritbue** { **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.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# redistribute ospf 1 metric 10 level-1
```

Related Commands

Command	Description
redistribute isis [**tag**] **level-2 into level-1**	Redistribute the reachable routing information from Level-2 into Level-1.
redistribute isis [**tag**] **level-1 into level-2**	Redistribute the reachable routing information from Level-1 into Level-2.

route-map	Configure the route map.

Platform Description N/A

4.52 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. The **no** form of this command cancels this redistribution.

redistribute isis [*tag*] **level-2 into level-1** [**route-map** *route-map-name* | **distribute-list** *access-list-name*]

no redistribute isis [*tag*] **level-2 into level-1** [**route-map** *route-map-name* | **distribute-list** *access-list-name*]

Parameter Description

Parameter	Description
tag	Name of the IS-IS instance to be redistributed.
route-map *route-map-name*	Set the route map during the route redistribution, which is used to filter the redistributed routes and set attributions of the routes. Name of the *route-map-name* shall not be over 32 characters. ● No route-map is configured by default.
distribute-list *access-list-name*	● Use 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>* | *acl-name*} ● In the IS-IS address-family ipv6 mode, you can use only the naming prefix list with the format being *acl-name.*

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 redistritbue isis** *tag1* l**evel-2 into level-1 route-map** *a* " will disable route-map aa filtering during redistribution instead of disabling the isis *tag1* redistribution.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis aa
Ruijie(config-router)# redistribute isis bb level-2 into level-1
```

Related Commands

Command	Description
redistribute	Redistribute the routing information from another routing protocol.
redistribute isis level-1 into level-2	Redistribute the reachable routing information from Level-1 into Level-2.

Platform Description N/A

4.53 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
tag	Name of the IS-IS instance.
route-map *route-map-name*	Set the route map during the route redistribution, which is used to filter the redistributed route and set attributions of this route. Name of the *route-map-name* shall not be over 32 characters. No **route-map** is configured by default.
distribute-list *access-list-name*	Use 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>* | *acl-name*} In the IS-IS **address-family ipv6** mode, you can use only the naming prefix list with the format being *acl-name.*

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 instace.

Command IS-IS routing process configuration mode or IS-IS **address-family ipv6** mode.

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 redistritbue isis** *tag1* l**evel-1 into level-2 route-map** aa " will disable route-map aa filtering during redistribution instead of disabling the isis tag1 redistribution.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis aa
Ruijie(config-router)# redistribute isis bb level-1 into level-2
```

Related Commands

Command	Description
redistribute	Redistribute the routing information from another routing protocol.
redistribute isis level-2 into level-1	Redistribute the reachable routing information from Level-2 into Level-1.

Platform Description N/A

4.54 router isis

Use this command to create the IS-IS instance. The **no** form of this command deletes this instance.
router isis [*tag*]
no router isis [*tag*]

Parameter Description

Parameter	Description
tag	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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
```

Related Commands

Command	Description
ip router isis	Enable the IS-IS IPv4 routing protocol on the interface.
ipv6 router isis	Enable the IS-IS IPv6 routing protocol on the interface.
net	Set the NET address.

Platform Description N/A

4.55 spf-interval

Use this command to set the minimal interval for the SPF calculation. Use the **no** form of this command to restore the minimal interval to the default value.
spf-interval [**level-1** | **level-2**] *interval*
no spf-interval

Parameter Description

Parameter	Description
interval	The minimal interval for the SPF calculation in the range of 1 to 120, with unit being second.

Defaults By default, this command is not configured.
The default SPF interval is 10 seconds, which takes effect on both Level-1 and Level-2.

Command Mode IS-IS routing process configuration mode

Usage Guide To avoid wasting the CPU resource due to the frequent SPF calculation, set and increase the SPF minimal interval. However, increasing the interval also causes the response to the routing change delayed.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# spf-interval level-1 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.56 summary-address

Use this command to configure the IPv4 aggregation route. The **no** form of this command deletes the aggregation route.

summary-address *address/prefix* [**level-1** | **level-2** | **level-1-2**]

no summary-address *address/prefix*

Parameter Description

Parameter	Description
address / prefix	Aggregation network address and the IP prefix length of the aggregation network address, in the format of A.B.C.D/<0-32>
level-1	Take effect on the Level-1only.
level-1	Take effect on the Level-2 only.
level-1-2	Take effect on both Level-1 and Level-2.

Defaults By default, no aggregation route is configured.
If the Level is not specifief, it is defaulted to take effect on the Level-2.

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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# summary-address 10.10.0.0/24 level-1-2
```

Related Commands

Command	Description
summary-prefix	Configure the IPv6 aggregation route.

Platform Description N/A

4.57 summary-prefix

Use this command to configure the IPv6 aggregation route. The **no** form of this command deletes the aggregation route.

summary-prefix *ipv6-prefix/prefix-length* [**level-1** | **level-2** | **level-1-2**]

no summary-address *ipv6-prefix/prefix-length* [**level-1** | **level-2** | **level-1-2**]

Parameter Description

Parameter	Description
ipv6-prefix / prefix-length	Aggregation network address and the IP prefix length of the aggregation network address.
level-1	Take effect on the Level-1 only.
level-2	Take effect on the Level-2 only.
level-1-2	Take effect on both Level-1 and Level-2.

Defaults By default, no aggregation route is configured.
If the Level is not specified, it is defaulted to take effect on the Level-2.

Command Mode Address-family ipv6 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 Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# address-family ipv6
Ruijie (config-router-af)# summary-prefix 1000::/96 level-1-2
```

Related Commands

Command	Description
summary-address	Configure the IPv4 aggregation route.

Platform Description N/A

4.58 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
system-id	Additional system ID. The length is 6 bytes.

Defaults No additional system ID is configured by default.

Command Mode IS-IS routing process configuration 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 Examples The following example configures an additional system ID for fragment extension.

```
Ruijie(config)# router isis
Ruijie(config-router)# virtual-system 0000.0000.0034
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.59 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
vrf-name	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:

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.

An IS-IS process can be bound with only one VRF instance. A VRF instance can be bound with multiple IS-IS processes.

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 Examples The following example binds an IS-IS process with a VRF instance.

```
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

4.60 show clns is-neighbor

Use this command to show all IS neighbors to provide the adjacency relationship of routers.
show clns [*tag*] **is-neighbors** [*IFNAME* | **detail**]

Parameter Description

Parameter	Description
tag	Specify the IS-IS instance.
IFNAME	Specify the name of interface.
detail	Show detailed information of all interfaces.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration Examples The output results of the **show clns is-neighbors detail** command are shown 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	Show all IS neighbors to provide the router information and the adjacency relationship of terminal system.

Platform Description N/A

4.61 show clns neighbors

Use this command to show all IS neighbors to provide the router information and the adjacency relationship of terminal system.

show clns [*tag*] **neighbors** [*IFNAME* | **detail**]

Parameter Description

Parameter	Description
tag	Specify the IS-IS instance.
IFNAME	Specify the name of the interface.
detail	Show detailed information of all interfaces.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The output results of the **show clns neighbors detail** command are shown as below:

```
Area (null):
System Id     SNPA             State  Holdtime  Type Protocol
Interface
r1            00d0.f822.33ad    Up    7         L1   IS-IS
VLAN 1
Up    7         L2   IS-IS
VLAN 1
  Adjacency ID: 1
  Uptime: 00:02:47
  Area Address(es): 49.1111
```

Related Commands

Command	Description
show clns is-neighbors	Show all IS neighbors to provide the router adjacency relationship.

Platform Description N/A

4.62 show isis counter

Use this command to show various statistics of IS-IS.

show isis [*tag*] **counter**

Parameter Description

Parameter	Description
tag	Specify the IS-IS instance.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The output results of the **show clns neighbors details** are shown 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 Description N/A

4.63 show isis database

Use this command to show the LSP database.

show isis [*tag*] **database** [*FLAGS* | *LEVEL* | *LSPID*]

Parameter Description

Parameter	Description
tag	Specify the IS-IS instance.
FLAGS	The format is shown as below: detail verbose detail: detailed information Verbose: more detailed information than the detail.
LEVEL	The format is shown 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
LSPID	Specify the ID number of LSP to show the corresponding LSP information only.

Defaults N/A

Command Mode Privileged EXEC mode/ global configuration mode

Usage Guide N/A

Configuration Examples The output results of the **show isis database detail** command are shown as below:

```
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 Description N/A

4.64 show isis graceful-restart

Use this command to show 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

Usage Guide N/A

Configuration Examples The following example shows the GR information of the IS-IS default instance in the global configuration mode.

```
Ruijie(config)# show isis graceful-restart
Graceful-restart: enabled, graceful-period: 60s, Level timer: 60, Interface
timer: 3s.
Graceful-restart Helper: enabled.
```

Related Commands	Command	Description
	graceful-restart	Enable the IS-IS GR Restart capability.

graceful-restart grace-period	Configure the maximum interval of the grace-restart.
graceful-restart helper disable	Disable the IS-IS GR Help capability.
graceful-restart	Enable the IS-IS GR Restart capability.

Platform Description N/A

4.65 show isis hostname

Use this command to show the mapping relation between the router name and System ID.

show isis [*tag*] **hostname**

Parameter Description

Parameter	Description
tag	Specify the IS-IS instance.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The output results of the **show isis hostname** command are shown as below:

```
Ruijie# show isis hostname
System ID      Dynamic Hostname
5555.5555.5555 Ruijie
1111.1111.1111 r1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.66 show isis interface

Use this command to show the detailed information of IS-IS interface.

show isis [*tag*] **interface** [*IFNAME*]

Parameter

Parameter	Description

Description

tag	Specify the IS-IS instance name.
IFNAME	Specify the Interface name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The output results of the show isis interface command are shown as below:

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.67 show isis mesh-groups

Use this command to show the mesh-group configurations on each interface.

show isis [*tag*] **mesh-groups**

Parameter

Parameter	Description

Description

tag	Specify the IS-IS instance.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The output results of the **show isis mesh-groups** command are shown as below:

```
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 Description N/A

4.68 show isis neighbors

Use this command to show the IS-IS neighbors..

show isis [*tag*] **neighbors** [*detail*]

Parameter Description

Parameter	Description
tag	Specify the IS-IS instance.
detail	Show the detailed information of all interfaces.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The output results of the **show isis neighbors detail** command are shown as below:

```
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    VLAN 1
L2    1.0.0.2      Up      9         r1.01    VLAN 1
  Adjacency ID: 1
  Uptime: 00:06:25
  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
N/A	N/A

Platform Description N/A

4.69 show isis topology

Use this command to show the topology of the IS-IS router connection.

show isis [*tag*] **topology** [**l1** | **l2** | **level-1** | **level-2**]

Parameter Description

Parameter	Description
tag	Specify the IS-IS instance.
l1	Specify the topology of Level-1.
level-1	Specify the topology of Level-1.
l2	Specify the topology of Level-2.
level-2	Specify the topology of Level-2.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The output results of the **show isis topology** command are shown as below:

```
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   VLAN 1
```

```
Ruijie       --
IS-IS paths to level-2 routers
System Id    Metric   Next-Hop   SNPA             Interface
r1           10       r1         00d0.f822.33ad   VLAN 1
Ruijie       --
```

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** form of this command to exit BGP address configuration mode.

address-family ipv4 [unicast|multicast|mdt]

no address-family ipv4 [unicast|multicast|mdt]

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

Usage Guide

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**.
You can enter the multicast mode to configure the BGP of the multicast topology, which is used for RPF detection of the IPv4 multicast routing protocol.
You can enter mdt address family mode to configure the BGP of the multicast topology VPN, which is used for obtaining the cross-domain exit agent in the IPv4 multicast routing protocol.

Configuration Examples

The following example enters the IPv4 address family configuration mode.

```
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** form of this command to restore the default setting.

address-family ipv4 vrf *vrf-name*

no address-family vrf *vrf-name*

Parameter Description

Parameter	Description
vrf-name	VRF name

Defaults No vrf is defined by default.

Command Mode BGP configuration mode

Usage Guide You can execute this command to configure or exit the exchange of route information between PEs and CEs.
To return to BGP configuration mode, run the **exit-address-family** command.

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** 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**]

Parameter Description

Parameter	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

Usage Guide 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.

The **exit-address-family** command is used to return to BGP configuration mode.

Configuration Examples

The following example enters the IPv6 address family configuration mode.

```
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** 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*

Parameter Description

Parameter	Description
vrf-name	VRF name

Defaults

No vrf address family is defined by default.

Command Mode

BGP configuration 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 Examples

The following example enters the IPv6 VRF address family configuration mode.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv6 vrf vpn1
```

Configuration Examples

Command	Description
exit-address-family	Exits the mode.

Platform Description N/A

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.

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 The following example enters the L2VPN VPLS address family configuration mode.

```
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family l2vpn vpls
```

Related Commands

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 vpn4

Parameter Description

Parameter	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 Guide Use the **exit-address-family** command to exit the VPNv4 address family configuration mode.

Configuration Examples The following example enters the VPNv4 address family configuration mode.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family vpnv4
```

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 vpn4

Parameter Description

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 Guide Use the **exit-address-family** command to exit the VPNv6 address family configuration mode.

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** 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

Parameter Description

Parameter	Description
ip address	IP address of the aggregate route
mask	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.
map-tag	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
```

Related

Command	Description

Commands		
	router bgp	Enables the BGP protocol.

Platform Description None

5.9 aggregate-address (IPv6)

Use this command to set the aggregate IPv6 route. Use the **no** 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*

Parameter Description

Parameter	Description
ipv6-network	IP address prefix of the aggregate route
length	Length 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.
map-tag	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 or BGP IPv6 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 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 bfd bind bgp

Use this command to manually configure the BFD session for the BGP protocol. Use the **no** or **default** form of the command to restore the default setting.

bfd bind bgp peer-ip *ip-address* [**vrf** *vrf-name*] **interface** *interface-type interface-index* **source-ip** *ip-address*

no bfd bind bgp peer-ip *ip-address* [**vrf** *vrf-name*] **interface** *interface-type interface-index* **source-ip** *ip-address*

default bfd bind bgp peer-ip *ip-address* [**vrf** *vrf-name*] **interface** *interface-type interface-index* **source-ip** *ip-address*

Parameter Description

Parameter	Description
peer-ip *ip-address*	Peer IP address.
vrf *vrf-name*	The VRF instance where the BFD session is. The default is global VRF.
interface *interface-type interface-index*	Outbound interface type and its index.
source-ip *ip-address*	Local IP address.

Defaults No static BFD session is configured for BGP by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures a static BFD session for BGP.

```
Ruijie(config)# bfd bind bgp peer-ip 10.0.0.1 interface GigabitEthernet 0/1 source-ip 10.0.0.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.11 bgp advertise non-transitive extcommunity

Use this command to allow carried non-transitive extcommunty when BGP is notifying EBGP neighbors of a route. Use the **no** form of this command to restore the default setting.

bgp advertise non-transitive extcommunity

no bgp advertise non-transitive extcommunity

Parameter Description

Parameter	Description
N/A	N/A

Defaults Non-transitive extcommunty 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 extcommunty with the "non-transitive" flag. This configuration can enable the notification of non-transitive extcommunty.

Non-transitive extcommunty will be carried when notifying alliance EBGP or IBGP neighbors of a route.

Configuration Examples The following example allows carried non-transitive extcommunty.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp advertise non-transitive extcommunity
```

Configuration Examples

Command	Description
router bgp	Enables BGP protocol.

Platform Description N/A

5.12 bgp always-compare-med

Use this command to compare Multi Exit Discriminator (MED) all the time. Use the **no** form of this command to restore the default setting.

bgp always-compare-med

no 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
show ip bgp	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

5.13 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** form of this command to restore the default setting.

bgp asnotation dot

no bgp asnotation dot

Parameter Description

Parameter	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

Usage Guide

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.

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 Examples

The following example modifies the showing mode of the 4-byte AS notation.

```
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

5.14 bgp bestpath as-path ignore

Use this command to disregard the length of the AS path. Use the **no** form of this command to restore the default setting.

bgp bestpath as-path ignore

no 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

Command	Description

Commands		
	show ip bgp	Displays the BGP route entry.

Platform Description None

5.15 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** form of this command to restore the default setting.

bgp bestpath as-path multipath-relax

no 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.

```
Ruijie(config)# router bgp 65530
Ruijie(config-router)# bgp bestpath as-path multipath-relax
```

Related Commands

Command	Description
router bgp	Enables BGP.
show ip bgp	Displays BGP routing entries.

Platform Description None

5.16 bgp bestpath compare-confed-aspath

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** form of this command to restore the default setting.

bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

Parameter Description

Parameter	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

5.17 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** form of this command to restore the default setting.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Parameter Description

Parameter	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 Guide 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 Examples The following example compares the router ID of the same external routes.

```
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

5.18 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** form of this command to restore the default setting.

bgp bestpath med confed [missing-as-worst]

no 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 Guide The MED attribute of the path is transferred between the ASs inside the confederation. You may set always comparing this value.

Configuration Examples The following example compares the MED value of the path of the internal peer.

```
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

5.19 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** form of this command to restore the default setting.

bgp bestpath med missing-as-worst

no 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 None

Description

5.20 bgp client-to-client reflection

Use this command to enable the route reflection function between clients on the device. Use the **no** form of this command disables the route reflection function between clients.

bgp client-to-client reflection

no bgp client-to-client reflection

Parameter Description

Parameter	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

5.21 bgp cluster-id

Use this command to configure the cluster ID of the route reflector. Use the **no** form of this command to restore it to the default setting.

bgp cluster-id *cluster-id*

no bgp cluster-id

Parameter Description

Parameter	Description
cluster-id	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 Guide 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.

Configuration Examples The following example configures the cluster ID of the route reflector.

```
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

5.22 bgp confederation identifier

Use this command to configure the AS confederation identifier. Use the **no** form of this command to restore the default setting.

bgp confederation identifier *as-number*

no bgp confederation identifier

Parameter Description

Parameter	Description
as-number	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 BGP configuration mode

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 Examples

The following example configures the AS confederation identifier.

```
Ruijie(config-router)# bgp confederation identifier 65000
```

Related Commands

Command	Description
bgp confederation peers	Adds member AS of the AS confederation.

Platform Description

None

5.23 bgp confederation peers

Use this command to configure member ASs of the AS confederation. Use the **no** form of this command to restore the default setting.

bgp confederation peers *as-number* […*as-number*]

no bgp confederation peers *as-number* […as-number]

Parameter Description

Parameter	Description
as-number	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

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 Examples

The following example configures member ASs of the AS confederation.

```
Ruijie(config-router)# bgp confederation peers 65000 65100
```

Related Commands

Command	Description
bgp confederation identifier	Configures the confederation identifier.

Platform Description

None

5.24 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** form of this command to restore the default setting.

bgp dampening [*half-life* [*reusing suppressing duration*] | **route-map** *name*]

no bgp dampening

Parameter Description

Parameter	Description
half-life	Half-life period, ranging from 1 to 45 minutes
reusing	When the penalty value reaches this value, the routing suppression is cancelled. The value ranges from 1 to 20000.
suppressing	When the penalty value reaches this value, routing is suspended. The value ranges from 1 to 20000.
duration	Maximum time for routing suppression, ranging from 1 to 255 minutes
name	Route-map name, apply the routing attenuation to the specified route through the route-map.

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.

Configuration Examples

The following example enables the routing attenuation and set the attenuation parameters.

```
Ruijie(config-router)# bgp dampening 30 1500 10000 120
```

Related Commands

Command	Description
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

5.25 bgp default ipv4-unicast

Use this command to set the IPv4 unicast address as the default address family. Use the **no** form of this command to restore the default setting.

bgp default ipv4-unicast

no 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

Usage Guide

This command is used to set the default address family of BGP as the IPv4 unicast address.

Configuration Examples

The following example sets the IPv4 unicast address as the default address family.

```
Ruijie(config-router)# default ipv4-unicast
```

Related Commands

Command	Description
address-family ipv4	Enters the IPv4 address mode.

Platform Description

None

5.26 bgp default local-preference

Use this command to set the default local-preference attribute value. Use the **no** form of this command to restore the default setting.

bgp default local-preference *value*

no bgp default local-preference

Parameter Description

Parameter	Description
value	Local priority attribute, in the range from 0 to 4294967295

Defaults The local preference value is 100 by default.

Command Mode BGP configuration mode, BGP IPv4 VRF address-family configuration mode or BGP IPv6 VRF address-family configuration mode.

Usage Guide 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. The BGP speaker sends the external route received to the IBGP peers to add the local priority value.

Configuration Examples The following example sets the default local-preference attribute value.

```
Ruijie(config-router)# bgp default local-preference 200
```

Related Commands

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

5.27 bgp default route-target filter

Use this command to enable the route-targe filtering. For the VPNV4 routes, filter the community attributes of the route-targe by default. Use the **no** form of this command to disable this function.

bgp default route-targe filter

no bgp default route-targe filter

Parameter

Parameter	Description

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-targe 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-targe of local VRF. With the PE route-reflector-client configured for the BGP, the VPNV4 route will not be processed through the route-targe filtering. In this case, whether the BGP is enabled, the actions are the same without the route-targe filtering.

Configuration Examples The following example enables the route-targe filtering.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# no bgp default route-targe 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

5.28 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** form of this command to restore the default setting.

bgp deterministic med

no bgp deterministic med

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP configuration mode

Usage They will be compared with each other according to the sequence the paths are received when the

Guide 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

5.29 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** form of this command to disable this function.

bgp enforce-first-as

no bgp enforce-first-as

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode BGP configuration mode

Usage Guide The AS number of the device is put into the path section by default to update the update message.

Configuration Examples The following example rejects the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number.

```
Ruijie(config-router)# bgp enforce-first-as
```

Related Commands

Command	Description
show ip bgp	Displays the BGP route entry.

Platform None

Description

5.30 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** form of this command to disable this function.

bgp fast-external-fallover

no bgp fast-external-fallover

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode BGP configuration mode

Usage Guide This command takes effect only for the directly-connected EBGP neighbor.

Configuration Examples The following example creates the fast BGP session.

```
Ruijie(config-router)# bgp faster-external-fallover
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

Platform Description None

5.31 bgp fast-route

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 Description

Parameter	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

5.32 bgp graceful-restart

Use this command to enable the global BGP graceful restart function. Use the **no** form of this command to disable BGP graceful restart.

bgp graceful-restart

no bgp graceful-restart

Parameter Description

Parameter	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

Usage Guide 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.

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

5.33 bgp graceful-restart disable

Use this command to disable GR capability of a BGP address family. Use the **no** form of this command to restore the default setting.

bgp graceful-restart disable

no bgp graceful-restart disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The function is disabled 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 enables the graceful restart function of the global BGP.

```
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

5.34 bgp graceful-restart restart-time

Use this command to configure the restart time of the BGP graceful-restart. Use the **no** form of this command to restore the default setting.

bgp graceful-restart restart-time *restart-time*

no bgp graceful-restart restart-time

Parameter Description

Parameter	Description
restart-time	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.

Defaults

The default is 120.

Command Mode

BGP configuration mode.

Usage Guide

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.

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.

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 restart-time 150
Ruijie(config-router)# no bgp graceful-restart restart-time
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform Description

N/A

5.35 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** form of this command to restore the default setting.

bgp graceful-restart stalepath-time stalepath-time *time*

no bgp graceful-restart stalepath-time

Parameter Description

Parameter	Description
time	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
Ruijie(config-router)# no bgp graceful-restart stalepath-time
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform Description

N/A

5.36 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* [*starup-time*]

no bgp initial-advertise-delay

default bgp initial-advertise-delay

Parameter Description

Parameter	Description
delay-time	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.
startup-time	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.

Defaults

The initial advertisement delay is disabled by default.

Command Mode

BGP configuration mode

Usage Guide

When BGP is started, it waits a specified period of time (delay time) for its neighbors to be established themselves and to begin sending their initial updates. Once that period is complete, or when the time expires, the software starts sending advertisements out to its peers. After that, BGP sends the updates at the interval configured through the **neighbor advertisement-interval** command. The startup-time is the time that the device startup. In the period of startup-time, BGP waits the delay-time before sending its updates. This command enables the BGP peers to change the neighbor update advertisement after restart.

The **bgp initial-advertise-delay** command is used to tune the initial delay period before a BGP device sends its first updates depending on the hardware limitation, the number of neighbors and routes.

Configuration Examples

The following example configures initial delay to 60 seconds within 500 seconds after BGP restart.

```
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 Description

N/A

5.37 bgp log-neighbor-changes

Use this command to log the BGP status changes without turning on debug. Use the **no** form of this command to disable this function.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

BGP configuration mode

Usage Guide

The debug command can also be used to log BGP status changes. But this command may consume many resources.

Configuration Examples

The following example logs the BGP status changes without turning on debug.

```
Ruijie(config-router)# bgp log-neighbor-changes
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

Platform Description

None

5.38 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

Parameter	Description
number	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 Guide 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 Examples The following example sets the maximum number of ASs in the BGP AS-PATH attribute to 100.

```
Ruijie(config-router)# bgp maxas-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.39 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** form of this command to restore the default setting.

bgp mp-error-handle session-retain [**recovery-time** *time*]

no bgp mp-error-handle session-retain

Parameter Description

Parameter	Description
recovery-time *time*	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

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 t 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

5.40 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** form of this command to restore the default setting.

bgp nexthop trigger delay *delay-time*

no bgp nexthop trigger delay

Parameter Description

Parameter	Description
delay-time	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 Mode BGP configuration mode, IPv4/IPv6/VPNv4 address family configuration mode, IPv4 VRF address family configuration mode

Usage Guide 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.

Configuration Examples The following example retains BGP sessions when BGP protocol detects errors in multi-protocol route attributes.

```
Ruijie(config-router)# bgp nexthop trigger delay 30
```

Related Commands	Command	Description
	bgp nexthop trigger enable	Enables the nexthop trigger.

Platform Description None

5.41 bgp nexthop trigger enable

Use this command to enable the nexthop trigger update function. Use the **no** form of this command to disable this function.

bgp nexthop trigger enable

no bgp nexthop trigger enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Mode BGP configuration mode, IPv4/IPv6/VPNv4 address-family configuration mode, BGP IPv4 VRF address-family configuration mode or BGP IPv6 VRF address-family 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.

```
Ruijie(config-router)# bgp nexthop trigger enable
```

Related Commands	Command	Description
	Bgp nexthop trigger delay	Sets the delay time for updating the routing table when the nexthop changes.

Platform Description None

5.42 bgp notify unsupport-capability

Use this command to enable the neighbor address family capability detection function. Use the **no** form of this command to restore the default setting.

bgp notify unsupport-capability

no bgp notify unsupport-capability

Parameter	Parameter	Description

Description

N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP 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 unsupport-capability
```

Configuration Examples

Command	Description
router bgp	Enables BGP protocol.

Platform Description N/A

5.43 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** form of this command to disable this function.

bgp redistribute-internal

no 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 address family configuration mode, IPv4 VRF address family 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
```

Related Commands	Command	Description
	redistribute	Redistributes routes learned from other protocols.

Platform Description None

5.44 bgp router-id

Use this command to configure the ID-IP address of the device. Use the **no** form of this command to restore the default setting.

bgp router-id *ip-address*

no bgp router-id

Parameter Description	Parameter	Description
	ip address	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

Usage Guide This command is used to configure IP address, the ID of the device when running the BGP protocol.

Configuration Examples The following example configures the ID-IP address of the device.

```
Ruijie(config-router)# bgp router-id 10.0.0.1
```

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

5.45 bgp scan-rib disable

Use this command to update the routing table by event triggering. Use the **no** form of this command to restore the default setting.

bgp scan-rib disable

no 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/ IPv4/IPv6/VPNv4 address-family configuration mode/ IPv4 VRF address family configuration mode

Usage Guide N/A

Configuration Examples The following example configures the timely scan for the BGP protocol.

```
Ruijie(config-router)# bgp scan-rib disable
```

Related Commands

Command	Description
bgp scan-time	Configures the interval for the BGP timely scan.

Platform Description None

5.46 bgp scan-time

Use this command to configure the interval for the BGP timely scan. Use the **no** form of this command to restore the default setting.

bgp scan-time *time*

no bgp scan-time [*time*]

Parameter Description

Parameter	Description
time	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/ IPv4/IPv6/VPNv4 address family configuration mode/ IPv4 address-family VRF configuration mode and IPv6 VRF address family 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

5.47 bgp tcp-source-check disable

Use this command to configure BGP's TCP source check function. Use **no** form of this command to disable this function.

bgp tcp-source-check disable

no bgp tcp-source-check disable

Parameter Description	Parameter	Description
	-	-

Defaults This function is enabled by default.

Command Mode BGP 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.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp tcp-source-check disable
```

Configuration Examples	Command	Description
	router bgp	Enables BGP protocol.

Platform Description N/A

5.48 bgp timer accuracy-control

Use this command to configure BGP's internal timer accuracy control. Use **no** form of this command to restore the default setting.

bgp timer accuracy-control

no 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.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp timer accuracy-control
```

Configuration Examples

Command	Description
router bgp	Enables BGP protocol.

Platform Description N/A

5.49 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** 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

Parameter Description

Parameter	Description
delay-time	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

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.

Configuration Examples

The following example sets the update-delay time to 200 seconds.

```
Ruijie(config)# router bgp 500
Ruijie(config-router)# bgp graceful-restart
Ruijie(config-router)# bgp update-delay 200
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful-restart.

Platform Description

None

5.50 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 Description

Parameter	Description
af-mode	CLI is displayed in address family configuration mode.
scope-mode	CLI is displayed in scope configuration mode.

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 Examples The following example sets the scope global configuration mode as the BGP CLI display mode.

```
Ruijie(config)# router bgp 500
Ruijie(config-router)# bgp upgrade-cli scope-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.51 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
none parameter	Resets peer sessions in all address-families.
as-number	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 Guide This command is used to reset sessions of all supported address-families, including the vrf session in every address-family.

Configuration Examples N/A

Related Commands

Command	Description
clear bgp ipv4 unicast	Resets the IPv4 unicast address-family.

Platform Description None

5.52 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
peer-group-name	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 -

5.53 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
vrf-name	VRF name
*	Resets all peer group sessions under address families.
as-number	Resets sessions with all members in the specified AS.
peer-address	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 Description N/A

5.54 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
vrf-name	VRF name.
-	Clears the flap information of all routes.
address	IP address
mask	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 Examples The following example clears the flap information and disables route dampening.

```
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 and sets the dampening parameters.

Platform Description None

5.55 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
vrf-name	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 Examples The following example resets all EBGP connections.

```
Ruijie# clear bgp ipv4 unicast external in
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp neighbors	Displays the neighbor information.

Platform Description None

5.56 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
vrf-name	VRF name.
-	Clears all route flap information
address	IP address
mask	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 Examples The following example clears the route flap information.

```
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

5.57 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
vrf-name	VRF name
peer-group-name	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 Examples The following example resets the session with all members in the peer group.

```
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

5.58 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
vrf-name	VRF name

Defaults -

Command Mode Privileged EXEC 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 -

5.59 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
vrf-name	VRF name
*****	Resets all peer group sessions under address families.
as-number	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.
peer-address	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 -

5.60 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
vrf-name	VRF name
-	Clears all routes' flap information.
ip-address	IP address
mask	Mask code

Defaults -

Command Mode Privileged EXEC 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 Examples The following example clears flap information and disables route dampening.

```
Ruijie# clear bgp ipv6 unicast dampening 192.168.0.0 255.255.0.0
```

Configuration Examples

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform Description -

5.61 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
vrf-name	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.

```
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

5.62 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
vrf-name	VRF name
-	Clears all route information's flap information.
address	IP address
mask	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 ipv4 unicast dampening** command.

Configuration Examples The following example clears IPv6 unicast address families' route flap statistics.

```
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 -

5.63 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

Parameter	Description

Description

vrf-name	VRF name
peer-group-name	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 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 -

5.64 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
vrf-name	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 -

5.65 clear bgp l2vpn vpls

Use this command to reset BGP's 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.
as-number	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.
peer-address	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 -

5.66 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.
ve_id:offset	Clears specified ve_id:offset'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 -

5.67 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 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 VPLS address families.

```
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 -

5.68 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.
ve_id:offset	Clears specified ve_id:offset'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.

```
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 -

5.69 clear bgp l2vpn vpls peer-group

Use this command to reset sessions with all members in the peer group.

clear bgp l2vpn vpls peer-group *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
peer-group-name	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 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 -

5.70 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.
as-number	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.
peer-address	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
clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.

Platform Description -

5.71 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.
ve_id:offset	Clears specified ve_id:offset'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 vpws dampening
```

Configuration Examples

Command	Description
bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform Description -

5.72 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.

```
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 -

5.73 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.
ve_id:offset	Clears specified ve_id:offset'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 -

5.74 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
peer-group-name	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
clear ip bgp	Resets BGP sessions.
show ip bgp	Displays BGP route entries.

Platform Description -

5.75 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.
as-number	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.
peer-address	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 -

5.76 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.
ip-address	IP address
mask	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 -

5.77 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.

```
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 -

5.78 clear bgp vpnv4 unicast flap-statistics

Use this command to clear VPNv4 address families' route flap statistics.

clear bgp vpnv4 unicast flap-statistics [*address* [*mask*]]

Parameter Description

Parameter	Description
-	Clears all routes' flap information.
address	IP address
mask	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.

```
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 -

5.79 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
peer-group-name	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 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 -

5.80 clear bgp vpnv6 unicast

Use this command to reset BGP's VPNv6 unicast address families.

clear bgp vpnv6 unicast { ***** | *as-number* | *peer-address* } [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
*****	Resets all peer group sessions under address families.
as-number	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, the device supports 4-byte AS number. The new AS number ranges from 1 to 4294967295, or from 1 to 65535.65535 in the dotted mode.
peer-address	Resets sessions with the specified peer.
in	Soft-resets the received route information.
out	Soft-resets the allocated route information.
soft	Soft-resets the received and sent route information.
soft in	Soft-resets the received route information.
soft out	Soft-resets the allocated route information.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is similar to the **clear bgp ipv4 unicast** command.

Configuration Examples N/A

Configuration Examples

Command	Description
N/A	N/A

Platform Description N/A

5.81 clear bgp vpnv6 unicast dampening

Use this command to clear flap information and disable route dampening.

clear bgp vpnv6 unicast dampening

Parameter Description

Parameter	Description

N/A	N/A

Defaults N/A

Command Mode Privileged EXEC 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 Examples The following example s clears BGP's route flap information and disables route dampening.

```
Ruijie# clear bgp vpnv6 unicast dampening
```

Configuration Examples

Command	Description
N/A	N/A

Platform Description N/A

5.82 clear bgp vpnv6 unicast external

Use this command to reset all EBGP connection of VPNv6 address family.

clear bgp vpnv6 unicast external [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description
-	Resets all BGP session.
in	Resets the received route information.
out	Resets the allocated route information.
soft	Soft-resets the received and sent route information.
soft in	Soft-resets the received route information.
soft out	Soft-resets the allocated route information.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example resets all EBGP connection of VPNv6 address family.

```
Ruijie# clear bgp vpnv6 unicast external in
```

Configuration Examples

Command	Description
N/A	N/A

Platform Description N/A

5.83 clear bgp vpnv6 unicast flap-statistics

Use this command to clear VPNv6 address family's route flap statistics.

clear bgp vpnv6 unicast flap-statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command clears only statistics of routes that are not dampened and does not disable route dampening. If you want to clear all route statistics and disable route dampening, use the **clear bgp vpnv6 unicast dampening** command.

Configuration Examples The following example clears VPNv6 address family's route flap statistics.

```
Ruijie# clear bgp vpnv6 unicast flap-statistics
```

Configuration Examples

Command	Description
N/A	N/A

Platform Description N/A

5.84 clear bgp vpnv6 unicast peer-group

Use this command to reset sessions with all members in the peer group.

clear bgp vpnv6 unicast peer-group *peer-group-name* [**soft**] [**in** | **out**]

Parameter Description

Parameter	Description

peer-group-name	Peer group name
in	Resets the received route information.
out	Resets the allocated route information.
soft	Soft-resets the received and sent route information.
soft in	Soft-resets the received route information.
soft out	Soft-resets the allocated route information.

Defaults N/A

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 the received route information with all members in the peer group called **my-group.**

```
Ruijie# clear bgp vpnv4 unicast peer-group my-group in
```

Configuration Examples

Command	Description
N/A	N/A

Platform Description N/A

5.85 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

Parameter	Description
vrf-name	VRF name.
*	Resets all the current BGP sessions and the OVERFLOW status of BGP ipv4 unicast address family.
address	Resets the BGP session with the specified peer.
as number	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.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

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.

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 Examples The following example resets the BGP session.

```
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

5.86 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
vrf-name	VRF name
address	IP address

mask	Mask

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide 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.

Configuration Examples The following example clears the dampening information and disables route dampening.

```
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

5.87 clear ip bgp external

Use this command to reset all EBGP connections.

clear ip bgp [vrf *vrf-name*] external [soft] [in | out]

Parameter Description

Parameter	Description
vrf-name	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 Examples The following example resets all EBGP connections.

```
Ruijie# clear ip bgp external in
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp neighbors	Displays the neighbor information.

Platform Description None

5.88 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

Parameter	Description
vrf-name	VRF name.
address	IP address
Mask	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 Examples The following example clears the routes vibration statistics of the IPv4 unicast address family.

```
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

5.89 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
vrf-name	VRF name.
peer-group-name	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 Guide This command resets the BGP session with all members in the peer group.

Configuration Examples The following example resets the session with all members in the peer group.

```
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

5.90 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 Description

Parameter	Description
vrf-name	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 Examples

The following example updates the table-map's route information applied by IPv4 unicast address family.

```
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

5.91 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 Description

Parameter	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

5.92 default-metric

Use this command to set the metric for route redistribution. Use the **no** form of this command to restore the default setting.

default-metric *number*

no default-metric

Parameter Description

Parameter	Description
number	Metric number, in the range from 1 to 4294967295

Defaults No metric is set by default.

Command Mode BGP configuration mode and various address-family configuration modes

Usage Guide

This command sets the metric of routes to be redistributed for integrity.

The metric set by the command cannot cover that set by the r**edistribute metric** command. The value is 0 when the default metric applies to redistributed connected routes.

Configuration Examples The following example sets the metric for route redistribution.

```
Ruijie(config-router)# default-metric 45
```

Related Commands

Command	Description
redistribute	Redistributes routes of other protocol.

Platform Description None

5.93 distance bgp

Use this command to set different management distances for different types of BGP routes. Use the **no** form of this command to restore the default setting.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Parameter Description

Parameter	Description
external-distance	Route management distance learned from EBGP peers, in the range from 1 to 255

internal-distance	Route management distance learned from IBGP peers, in the range from 1 to 255
local-distance	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

Defaults

The parameter defaults are as follows:
external-distance - 20
internal-distance - 200
local-distance - 200

Command Mode

BGP configuration mode, BGP IPv4 unicast address family configuration mode, BGP IPv4 multicast address family configuration mode, BGP IPv4 VRF configuration mode, BGP IPv6 VRF configuration mode, BGP IPv6 unicast address family configuration mode, BGP IPv6 multicast address family configuration mode.

Usage Guide

It is not recommended to change the management distance of the BGP route. If it is necessary, observe the following points:

- 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

5.94 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 Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode.

Platform Description None

5.95 maximum-paths ebgp

Use this command to configure the number of cost-equal paths for the EBGP multipathing load balancing function. Use the **no** form of this command to restore the default setting.

maximum-paths ebgp *number*

no maximum-paths ebgp

Parameter Description

Parameter	Description
number	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 Description N/A

5.96 maximum-paths ibgp

Use this command to configure the number of cost-equal paths for the IBGP multipathing load balancing function. Use the **no** form of this command to disable the IBGP multipathing load balancing function.

maximum-paths ibgp *number*

no maximum-paths ibgp

Parameter Description	Parameter	Description
	number	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 address-family configuration mode/ BGP IPv6 address-family 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

5.97 maximum-prefix

Description

Use this command to limit the maximum number of prefixes in the routing database in the address family. Use the **no** form of this command to restore the default setting.

maximum-prefix *maximum*

no maximum-prefix [*maximum*]

Parameter Description

Parameter	Description
maximum	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 address family configuration mode/ BGP IPv4 VRF configuration mode/ BGP IPv6 VRF configuration mode, BGP VPNv4 configuration mode/ BGP IPv4 MDT address family mode

Usage Guide

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.

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 vpnv4 unicast	Resets BGP's vpnv4 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 vpnv4 summary	Displays summary of BGP's vpnv4 unicast address families.

Platform Description

N/A

5.98 neighbor activate

Use this command to activate the neighbor or peer group in the current address mode. Use the **no** form of this command to disable this function.

neighbor {*peer-address* | *peer-group-name*} **activate**

no neighbor {*peer-address* | *peer-group-name*} **activate**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	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/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode / address-family VPNv4 configuration mode

Usage

The function is enabled by default for IPv4 address families. You need to set this command in other

Guide address-family configuration modes for exchanging routes.

Configuration Examples

The following example activates the neighbor or peer group in the current address mode.

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router)# address-family vpnv4
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

5.99 neighbor advertisement-interval

Use this command to set the time interval to send the BGP route update message. Use the **no** 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**

Parameter Description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
seconds	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 VRF configuration mode / BGP IPv6 VRF address family 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.

Configuration Examples

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

Command	Description

Commands		
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.

Platform Description None

5.100 neighbor allowas-in

Use this command to allow the PE to receive messages with the same AS number as itself. Use the **no** 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**

Parameter Description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Number of the AS number duplication in the range from 1 to 10, 3 by default

Defaults This function is disabled by default.

Command Mode BGP configuration mode/ IPv4 address family configuration mode/ IPv4 VRF address family configuration mode / IPv6 VRF address family 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

5.101 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
peer address	IP address of the peer.
peer-group-name	Name of the peer group, containing up to 32 characters.
seconds	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

5.102 neighbor as-override

Use this command to allow the PE to override the AS number of a site. Use the **no** 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**

Parameter Description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP IPv4 VRF address family configuration mode/ BGP IPv6 VRF address family configuration mode

Usage Guide

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.

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.

Configuration Examples

The following example allows the PE to override the AS number of a site.

```
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

5.103 neighbor default-originate

Use this command to allow the BGP speaker to advertise the default route to the peer (group). Use the **no** 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*]

Parameter Description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
map-tag	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 address family configuration mode, BGP IPv4 multicast address family configuration mode, BGP IPv4 VRF address family configuration mode, BGP IPv6 VRF address family configuration mode, BGP IPv6 unicast address family configuration mode and BGP IPv6 multicast address family 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.

Configuration Examples

The following example allows the BGP speaker to advertise the default route to the 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 default-originate
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

None

5.104 neighbor description

Use this command to set a descriptive sentence for the specified peer (group). Use the **no** 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**

Parameter Description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
text	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 VRF address family configuration mode and BGP IPv6 VRF address family configuration mode.

Usage Guide

This command is used to add descriptive characters for the peer (group). This may help remember features and characteristics of the peer (group).

Configuration Examples

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
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description None

5.105 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** 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**}

Parameter Description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
access-list-number	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/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ BGP IPv4 VRF configuration mode/ BGP IPv6 VRF address family configuration mode/ BGP VPNv4 address family configuration mode.

Usage Guide

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.

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.

Configuration Examples

The following example implements the routing policy based on the ACL when receiving/sending route information from/to the specified BGP peer.

```
Ruijie(config)# router bgp 60
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

5.106 neighbor ebgp-multihop

Use this command to allow establishing BGP connection between EBGP peers that are not directly connected. Use the **no** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*peer-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

Parameter Description

Parameter	Description
peer address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
ttl	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 ttl is 255.

Command Mode BGP configuration mode/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family 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.

Configuration Examples The following example allows establishing BGP connection between EBGP peers that are not directly connected.

```
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

5.107 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
peer address	IPv4 or IPv6 address of the peer.
peer-group-name	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

5.108 neighbor filter-list

Use this command to enable route filtering when sending/receiving routing information to/from BGP peers. Use the **no** 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**}

Parameter Description

Parameter	Description
peer address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
access-list-numbe	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/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode, IPv6 VRF address family configuration mode / address-family VPNv4 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
```

Related Commands

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 Description None

5.109 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** 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

Parameter	Description

Description

peer address	IP address of the peer, IPv4 address or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
as-number	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 options 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, IPv4 address family configuration mode, IPv6 address family configuration mode, IPv6 VRF address family configuration mode, IPv4 VRF address family configuration mode, and address-family VPNv4 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

5.110 neighbor maximum-prefix

Use this command to limit the number of prefixes received from the specified BGP peer. Use the **no** 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*

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
maximum	Upper limit of the number of the received route entries
threshold	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 address family configuration mode, BGP IPv6 address family configuration mode, BGP IPv4 VRF address family configuration mode, BGP IPv6 VRF address family configuration mode, BGP VPNv4 address family configuration mode, BGP L2VPN VPWS/VPLS address family 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 Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description None

5.111 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** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode

Usage Guide 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. 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
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description None

5.112 neighbor next-hop-unchanged

Use this command to maintain the next-hop when sending routes to the peer(group). Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	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/ IPv4 address family configuration mode/ BGP VPN 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

5.113 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** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
0	Displays the password with encryption.
7	Displays the password without encryption.
string	Password for MD5 authentication in the range from up to 80

	characters

Defaults The function is disabled by default

Command Mode BGP configuration mod, IPv4 address family configuration mode, IPv6 address family configuration mode, IPv4 VRF address family configuration mode, IPv6 VRF address family 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

5.114 neighbor peer-group (creating)

Use this command to create a BGP peer group. Use the **no** form of this command to restore the default setting.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

Parameter Description

Parameter	Description
peer-group-name	Name of the peer group of up to 32 characters

Defaults No BGP peer group is created.

Command Mode BGP configuration mode/ BGP IPv4 VRF configuration mode/ BGP IPv6 VRF address family 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
```

Related Commands

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 peer-group (assigning members)

Use this command to configure the specified peer as a member of the BGP peer group. Use the **no** 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*

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	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 VRF configuration mode/ BGP IPv6 VRF address family 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

The following example configures the specified peer as a member of the BGP peer group.

Examples

```
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
```

Related Commands

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

5.116 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** 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**}

Parameter Description

Parameter	Description
peer address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
prefix-lis-name	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/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode/ address-family VPNv4 configuration mode

Usage Guide

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.

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
```

Related Commands

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

5.117 neighbor remote-as

Use this command to configure the BGP peer (group). Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
as-number	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, IPv4 address family configuration mode, IPv6 address family configuration mode, IPv4 VRF address family configuration mode, IPv6 VRF address family 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

5.118 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 EBGP peer. Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode, IPv4 address family configuration mode, IPv6 address family configuration mode, IPv4 VRF address family configuration mode, IPv6 VRF address family configuration mode

Usage Guide

This command takes effect only on EBGP peers.
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
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description None

5.119 neighbor route-map

Use this command to enable route match for the received/sent routes. Use the **no** 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**}

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
map-tag	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, IPv4 address family configuration mode, IPv6 address family configuration mode, IPv4 VRF address family configuration mode, IPv6 VRF address family configuration mode, IPv4 VPNv4 address family configuration mode, BGP L2VPN VPLS/VPWS address family 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

5.120 neighbor route-reflector-client

Use this command to configure the local device as the route reflector and specifies its client. Use the **no** form of this command to restore the default setting.

neighbor *peer-address* **route-reflector-client**

no neighbor *peer-address* **route-reflector-client**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address

Defaults This function is disabled by default.

Command BGP configuration mode

Mode

Usage Guide

By default, all IBGP speakers in the autonomous system must establish neighbor relationship with 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

5.121 neighbor send-community

Use this command to transmit community attributes to the specified BGP neighbor. Use the **no** 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**]

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	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 Examples The following example transmits community attributes to the specified BGP neighbor.

```
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

5.122 neighbor send-label

Use this command to specify the device to send the route carrying the MPLS label to a neighbor. Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode, IPv4 address family configuration mode and IPv4 VRF address family 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

5.123 neighbor shutdown

Use this command to disconnect the BGP connection established with the specified BGP peer. Use the **no** form of this command to restore the default setting.

neighbor {*peer-address* | *peer-group-name*} **shutdown**

no neighbor {*peer-address* | *peer-group-name*} **shutdown**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters

Defaults This function is disabled by default.

Command Mode BGP configuration mode/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode

Usage Guide 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).
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
```

Related Commands

Command	Description
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

5.124 neighbor soft-reconfiguration inbound

Use this command to store the routing information sent from the BGP peer. Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	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

Usage Guide

This command restarts the BGP session, and keeps the unchanged routing information sent from the BGP peer (group).

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
```

Related Commands

Command	Description
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

5.125 neighbor soo

Use this command to set the SOO value of the neighbor. Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
soo-value	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 nnis defined by yourself. The range is from 0 to 65535. (3)soo_value = as4_num:nn an4_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 IPv4 VRF address family configuration mode/ IPv6 VRF address family 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 Examples The following example sets the SOO value of the neighbor.

```
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

5.126 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** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
keepalive	Time interval to send the KEEPALIVE message to the BGP peer. Range: 0-65535 seconds
holdtime	Time interval to consider the BGP peer alive Range: 0-65535 seconds
minimum-holdtime	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
minimum-holdtime: 0 seconds

Command Mode

BGP configuration mode, BGP IPv4 VRF address family configuration mode, BGP IPv6 VRF address family 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.

Configuration Examples

The following example sets the keepalive and holdtime time values used for establishing the BGP connection.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 80 240
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
timers bgp	Sets the keepalive and holdtime values globally.

Platform Description

None

5.127 neighbor unsuppress-map

Use this command to selectively advertise routing information suppressed by aggregate-address command. Use the **no** 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*

Parameter Description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
map-tag	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 Guide This command advertises the specified suppressed routes.
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 selectively advertises routing information suppressed by aggregate-address command.

```
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

5.128 neighbor update-source

In specifying the BGP peer to establish the BGP connection, use this command to set the network interface used for establishing the BGP connection. Use the **no** form of the command automatically to restore the default setting.

neighbor { *peer-address* | *peer-group-name* } **update-source** *interface-type interface-index*

no neighbor {*peer-address* | *peer-group-name*} **update-source**

Parameter Description

Parameter	Description
peer-address	IP address of the peer, IPv4 or IPv6 address
peer-group-name	Name of the peer group of up to 32 characters
interface-type	Interface type
interface-index	Interface index

Defaults The optimal local interface is used as the output interface by default.

Command Mode BGP configuration mode/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode

Usage Guide This command enables using the loopback interface to establish the BGP connection with BGP peer.
If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command.
If the peer initiates a connection, which interface is used for TCP connection will not be checked.

Configuration Examples The following example establishes the BGP connection.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 update-source lookback 1
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description None

5.129 neighbor version

Use this command to display the number of the BGP protocol version used by the specific BGP neighbor. Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	Version number

Defaults The default version number is 4.

Command Mode BGP configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP IPv6 VRF address family 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

5.130 neighbor weight

Use this command to set the weight for the specific neighbor. Use the **no** 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**

Parameter Description

Parameter	Description
peer-address	IP address of the peer
peer-group-name	Name of the peer group of up to 32 characters
number	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 Guide

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.
Executing the **set weight** command in the route map of the neighbor will overwrite this value.

Configuration Examples

The following example sets the weight for the specific neighbor.

```
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

5.131 network

Use this command to configure the network information to be advertised by the local BGP speaker.
Use the **no** 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**]

Parameter Description

Parameter	Description
network-number	Network number
mask	Subnet mask
map-tag	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/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family 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

5.132 network synchronization

Use this command to advertise the network information after the local BGP speaker is synchronized with the local device. Use the **no** form of this command to directly advertise the network information.

network synchronization

no network synchronization

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode BGP configuration mode/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family 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

5.133 overflow memory-lack

Use this command to allow BGP to enter the OVERFLOW state when the memory is insufficient. 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 Allow the BGP to enter the OVERFLOW state when the memory is insufficient.

Command Mode BGP configuration mode

Usage Guide

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.

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 Examples

The following example sets BGP not to enter the OVERFLOW configuration status when the memory is insufficient.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# no memory-lack overflow
```

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

5.134 redistribute

Use this to redistribute routes between the other routing protocol and the BGP. Use the **no** 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**]

Parameter

Parameter	Description

Description

protocol-type	The source protocol types for redistributing routes, including connected, static, RIP
route-map *map-tag*	Specifies the route map. No route map is associated with by default.
metric *metric-value*	Sets the default metric of the routes to be redistributed, null by default.

Defaults

This function is disabled by default.

Command Mode

BGP configuration mode, IPv4 address family configuration mode, IPv6 address family configuration mode, IPv4 VRF address family configuration mode, IPv6 VRF address family configuration mode

Usage Guide

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.

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

5.135 redistribute ospf

Use this command to redistribute routes between OSPF and BGP. Use the **no** 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**]}]

Parameter Description

Parameter	Description
process-id	OSPF process ID to be redistributed
route-map *map-tag*	Specifies the route map. No route map is associated by default.
metric *metric-value*	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/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode

Usage Guide

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.

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 Examples

The following example redistributes routes between OSPF and BGP.

```
Ruijie(config-router)# redistribute ospf 2 route-map static-rmap
Ruijie(config-router)# no redistribute ospf 4 match external rotue-map ospf-rmap
Ruijie(config-router)# no redistribute ospf 78
```

Related Commands

Command	Description
show ip protocol	Displays the protocol configuration.

Platform

None

Description

5.136 redistribute isis

Use this command to redistribute routes between ISIS and BGP. Use the **no** 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**]

Parameter Description

Parameter	Description
isis-tag	(Optional)ISIS process ID to be redistributed
route-map *map-tag*	Specifies the route map. No route map is associated by default.
metric *metric-value*	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, IPv4 address family configuration mode, or IPv6 address family configuration mode

Usage Guide

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.

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

5.137 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** form of this command to restore the default setting.

router bgp *as-number*

no router bgp *as-number*

Parameter Description

Parameter	Description
as-number	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 Examples The following example enables the BGP protocol.

```
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

5.138 synchronization

Use this command to enable the synchronization mechanism of BGP and IGP routing information. Use the **no** form of this command to restore the default setting.

synchronization

no synchronization

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP configuration mode, IPv4 address family configuration mode, IPv6 address family configuration mode

Usage Guide

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.

- 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

5.139 table-map

Use this command to control the route information distributed to the kernel table. Use the **no** form of this command to restore the default setting.

table-map *route-map-name*

no table-map

Parameter

Parameter	Description

Description	*route-map-name*	Name of the route-map

Defaults No table-map is configured by default,

Command Mode BGP configuration mode/ IPv4 address family configuration mode/ IPv6 address family configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family 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

5.140 timers bgp

Use this command to adjust the BGP network timer. Use the **no** form of this command to restore the default value.

timers bgp *keepalive holdtime* [*minimum-holdtime*]

no timers bgp

Parameter Description

Parameter	Description
keepalive	Time interval to send the keepalive message to the BGP peer Range: 0-65535 seconds.
holdtime	Time interval to consider the BGP peer alive Range: 0-65535 seconds.
Minimum-holdtime	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

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.

Configuration Examples

The following example adjusts the BGP network timer.

```
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

5.141 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

Parameter	Description
global	Global routing table.
vrf *vrf-name*	VRF name.

Defaults

No scope address family is defined by default.

Command Mode

BGP configuration mode.

Usage Guide

Enter the scope configuration mode to perform the configuration.
To exit the scope configuration mode, use the **exit** command.

⚠ 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 Description

N/A

5.142 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** | **filter-list** | **community-list** | **dampening** {**flap-statistics** | **dampened-paths**} | **regexp** | **quote-regexp** | **neighbors** {**received-routes** | **routes** | **advertised-routes**}]

Display the route dampening parameter.

show bgp all dampening parameters

Display the related information of the neighbors.

show bgp all neighbors.

show bgp all summary

Display the path information.

show bgp all paths

Parameter Description

Parameter	Description
Please refer to the detailed description of **show bgp ipv4 unicast** command.	Please refer to the detailed description of **show bgp ipv4 unicast** command.

Defaults

Please refer to the detailed description of **show bgp ipv4 unicast** command.

Command Mode

Privileged EXEC mode

Usage Guide

Please refer to the detailed description of **show bgp ipv4 unicast** command..

Configuration

None

Examples

Related Commands

Command	Description
show bgp ipv4 unicast	Displays the IPv4 unicast route information of BGP

Platform Description None

5.143 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*] 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**]

show bgp ipv4 unicast [vrf *vrf-name*] cidr-only

show bgp ipv4 unicast [vrf *vrf-name*] labels

Parameter Description

Parameter	Description
vrf-name	VRF name
network	Displays the specific routing information in the routing table
network-mask	Displays the routing information included in the specified network.
community *community-number*	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 *community-name*	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.
filter-list *path-list-number*	Displays the routing information matching the filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.
prefix-list *ip-prefix-list-name*	Displays the routing information matching the specified prefix-list.
quote-regexp *regexp*	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp *regexp*	Displays the BGP routing information with the AS path attribute matching the specified regexp.
route-map *map-tag*	Displays the routing information matching the specified route-map filtering condition.
neighbors *neighbor-address* **received-routes**	Displays all routing information received from the specified peer (including the accepted and refused route).
neighbors *neighbor-address* **routes**	Displays all the routing information received from the peer and accepted.
neighbors *neighbor-address* **advertised-routes**	Displays all the routing information sent to the specified peer.
cidr-only	Displays the routing information without the category.
labels	Displays the BGP-learnt and BGP-sent routes with the MPLS label.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide 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.

Configuration Examples

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 .*
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  nolabel/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

5.144 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
	vrf-name	VRF name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the IPv4 unicast route dampening parameters configured for BGP.

Configuration Examples

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
```

Related Commands N/A

Platform Description None

5.145 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

Parameter	Description
neighbor-address	Neighbor IPv4 address

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.

Configuration Examples

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
```

Related Commands N/A

Platform Description None

5.146 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 Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to view the path information in the route database.

Configuration Examples

The following example displays the path information of the IPv4 unicast in the route database.

```
Ruijie# show bgp ipv4 unicast paths
Address  Refcnt Path
[0x1d7806a0:0] (67)
[0x1d7389a0:13] (20) 10
```

Related Commands N/A

Platform Description None

5.147 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 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 IPv4 unicast.

Configuration Examples

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
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol

Platform Description None

5.148 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*]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
vrf-name	VRF name
IPv6-prefix	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>.
community *community-number*	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 *community-name*	Displays the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matches the community value or community-list.
dampening dampened-paths	Displays the restrained routing information.
dampening flap-statistics	Displays the routing dampening statistics.
filter-list *path-list-number*	Displays the routing information matching the filter-list.
inconsistent-as	Displays the routing information of the inconsistent source AS.
prefix-list *ipv6-prefix-list-name*	Displays the routing information matching the specified prefix-list.
quote-regexp *regexp*	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp *regexp*	Displays the BGP routing information with the AS path attribute matching the specified regexp.
route-map *map-tag*	Displays the routing information matching the specified route-map filtering condition.
neighbors *neighbor-address* **received-routes**	Displays all routing information received from the specified peer (including accepted and refused routes).
neighbors *neighbor-address* **routes**	Displays all the routing information received from the peer and accepted.
neighbors *neighbor-address* **advertised-routes**	Displays all the routing information sent to the specified peer.

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

5.149 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 Description

Parameter	Description
vrf-name	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

5.150 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 Description

Parameter	Description
vrf-name	VRF name
neighbor-address	Neighbor IPv6 address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to view the information of the connection with BGP IPv6 unicast neighbor. 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 neighbor-address	Displays the related information of BGP IPv4 unicast neighbor.

Platform Description None

5.151 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 Description

Parameter	Description
vrf-name	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.

Configuration Examples

The following example displays the path information of the IPv6 unicast in the route database.

```
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

5.152 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 Description

None

5.153 show bgp l2vpn

Use the following command to display the BGP L2VPN routing information.

show bgp l2vpn { **vpls | vpws** } **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 address family.

show bgp l2vpn { **vpls | vpws** } **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** } **all summary**

Use the following command to display the L2VPN information on the specified RD.

show bgp l2vpn { **vpls | vpws** } **rd** *vpn_rd* [*ve_id:offset*]

Use the following command to display the L2VPN information on the specified VFI.

show bgp l2vpn { **vpls | vpws** } **vfi** *vfi_name* [*ve_id:offset*]

Parameter Description

Parameter	Description
vpls	Displays VPLS information.
vpws	Displays VPWS information.
all	Displays all NLRI information that contains the VPLS instance or the VPWS instance.
ve_id:offset	Displays the VFI instance information of the specified ve_id:offset
neighbor [*peer-address*]	Displays the BGP L2VPN neighbor information. You can specify the specific neighbor information by entering the parameter *peer-address.* 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.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide 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
Origin codes: i - IGP, e - EGP, ? - incomplete

Network    Next Hop       Metric   LocPrf    Path
Route Distinguisher: 45000:100
*> 2:0     0.0.0.0                        ?
*> 100:3   172.168.201.2   0       100       ?
Route Distinguisher: 45000:200
*>01:10    0.0.0.0        0       32768     ?
*>i200:11  172.168.201.2   0       100       ?
```

The following example displays all L2VPN VPWS address family routing information.

```
Ruijie(config)# show bgp l2vpn vpws 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
Origin codes: i - IGP, e - EGP, ? - incomplete
Network    Next Hop       Metric   LocPrf    Path
Route Distinguisher: 45000:100
*> 3:0     0.0.0.0                        ?
*> 300:3   172.168.201.2   0       100       ?
Route Distinguisher: 45000:200
*>01:30    0.0.0.0        0       32768     ?
*>i300:11  172.168.201.2   0       200       ?
```

The following example displays the routing information of the BGP L2VPN address family 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

5.154 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
vpls	Displays VPLS information.
vpws	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 detail**	Displays detailed routing policy information on the BGP neighbor.
site-id *id*	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 Guide 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.

Configuration Examples

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
```

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. Connected; The remote site is connected with the local site. Unconnected: The remote site is not connected with the local site.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.155 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 [*network* | **neighbor** [| *address*] | **summary** | **label**]

show bgp vpnv4 unicast vrf *vrf_name* [*network* | **summary** | **label**]

show bgp vpnv4 unicast rd *rd_value* [*network* | **summary**| **label**]

Parameter Description

Parameter	Description
network	Network IP address
neighbor	Displays neighbor information.
summary	Displays the route summary information.
label	Displays the label information of routes.
vrf_name	VRF name
rd_value	RD value, for example, 100:1 or 202.118.239.165:1

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide This command is used to display the VPN information of all VRFs or RDs.

Configuration Examples

The following example displays the VPN or neighbor information of all the VRFs or RDs.

```
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
```

```
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

5.156 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 [*network* | **neighbor** [| *address* [**policy** [**detail**]]] | **summary** | **label**]

show bgp vpnv6 unicast vrf *vrf_name* [*network* | **summary** | **label**]

show bgp vpnv6 unicast rd *rd_value* [*network* | **summary**| **label**]

Parameter Description

Parameter	Description
network	Network IP address
neighbor [*address*]	Displays the BGP VPNv6 neighbor information. All BGP VPNv6 neighbor information is displayed by default.
neighbor *address* **policy**	Displays the summarized BGP neighbor routing policy.
neighbor *address* **policy detail**	Displays the detailed BGP neighbor routing policy.
summary	Displays the route summary information.
label	Displays the route label information.
vrf_name	VRF name
rd_value	RD value, for example, 100:1 or 202.118.239.165:1.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the VRF that supports IPv6 address family or the VPNv6 routing information of the RD.

Configuration Examples

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

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 : IBGP 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

5.157 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 [*network* [*network-mask*] | **cidr-only** | **community** | **filter-list** | **community-list** | **regexp** | **quote-regexp** | **extcommunity-list | inconsistent-as | labels | prefix-list | route-map | scan**]

Display route flap's parameters.

show ip bgp dampening { **flap-statistics** | **dampened-paths | parameters** }

Display neighbors' related information.

show ip bgp neighbors *peer-address* [**received-routes** | **routes** | **advertised-routes**]

show ip bgp summary

Display directory information.

show ip bgp paths

Display related information under VRF.

show ip bgp vrf *vrf-name*

Parameter Description

Parameter	Description
network	Displays specific route information in the route table.
network-mask	Displays route information in the specific network.
cidr-only	Displays route information without specific category.
community *community-number*	Displays route information containing specific community value. The *community-number* 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 *community-name*	Displays the BGP route information of the specified community list. The *community-name* 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 *path-list-number*	Displays the route information that complies with the filter list. The *path-list-numbe* 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 *peer-address*	Displays the route information of BGP neighbors.
paths	Displays the route information in the route database.
prefix-list	Displays the route information that complies with the prefix list.
quote-regexp *regexp*	Displays the BGP route information of regular expression in the specified double quotation mark of the AS route attribute.
regexp *regexp*	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.
vrf	Displays related information under BGP VRF.

Defaults -

Command Mode Privileged EXEC 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 -

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 *if-name*	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 Description N/A

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 *if-name*	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 Examples The following example clears the IPv6 PBR forwarded packet count.

```
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
route-map	Name of the route map

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.

Configuration Examples

The following examples send the packets with the source address 192.168.217.10 from the serial 2/0.

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)#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 ip next-hop	Defines the next hop of the policy-based routing.
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.

Platform Description

N/A

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 Description N/A

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
route-map	Name of the route map

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 ip next-hop	Defines the next hop of the policy-based routing.
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.

Platform Description N/A

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
route-map-name	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 displays 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.
route-map	Defines the route map for PBR.
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 Description

N/A

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 | redundance }

no ipv6 policy

Parameter

Parameter	Description

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.

Configuration Examples This function is valid for the multiple next-hops.
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 Description N/A

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
route-map-name	Name of the PBR router map applied locally, which is configured by the **router-map** command.

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

An IPv6 packet is received on the fastEthernet 0/0. If the packet is sent from 10::/64 network 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 Description

N/A

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 Examples The following example displays the correlation between the IPv4 policy router and BFD.

```
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 Description N/A

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 *if-name*	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 Examples The following example displays the IPv4 PBR information on the interfaces.

```
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.
VRF ID	Port-correlated VRF ID.
Route Flags	PBR flag bit: Route Type: “PBR” indicates PBR routes. “Normal” indicates common routes. Direct: PBR matching action, **permit** or **deny** Priority: PBR priority, **High** or **Low** Tos_Dscp: Displays whether the **tos** rule or the **dscp** rule is configured. Precedence: Displays whether the **set ip precedence** rule is configured.
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 Description N/A

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
route-map-name	The route-map name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv4 PBR route-map information.

```
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 Description N/A

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 *if-name*	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 Examples The following example displays the IPv4 PBR forwarded packet count.

```
Ruijie#show ip pbr statistics
IPv4 Policy-based route statistic
 gigabitEthernet 0/1
   statistics : 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
route-map-name	Specifies a route map to be applied on the interfaces.

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 Examples The following example displays the current PBR configured in the system.

```
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 Description N/A

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 Examples The following example displays the correlation between the IPv6 policy router and BFD.

```
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 *if-name*	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 Examples The following example displays the IPv6 PBR information on the interfaces.

```
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.
VRF ID	Port associated VRF ID.
Route Flags	PBR flag bit: Route Type: “PBR” indicates PBR routes. “Normal” indicates common routes. Direct: PBR matching action, permit or deny Priority: PBR priority, High or Low Tos_Dscp: Displays whether the tos rule or the dscp rule is configured. Precedence: Displays whether the set ip precedence rule is configured.
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 Description N/A

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
route-map-name	The route-map name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the IPv6 PBR route-map information.

```
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 *if-name*	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 Examples The following example displays the IPv6 PBR forwarded packet count.

```
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
route-map-name	Name of the PBR router map.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current PBR applied in the system.

```
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 Description N/A

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

string	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 Description N/A

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
vrf-name	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 Description N/A

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
vrf-name	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 Examples The following example adds an interface or sub-interface to a VRF.

```
Ruijie(config-if-GigabitEthernet 0/0)# ip vrf forwarding redvrf
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
vrf-name	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.

Platform Description N/A

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 Description

Parameter	Description
limit	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.
warn-threshold	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 *limit*, 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 vrf definition

Use this command to create the multiprotocol VRF.
vrf definition *vrf-name*

Parameter Description

Parameter	Description
vrf-name	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 Examples The following example s creates a multiprotocol VRF *vrf1.*

```
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 Description N/A

7.9 vrf forwarding

Use this command to bind a network interface to a multiprotocol VRF.
vrf forwarding *vrf-name*

Parameter Description

Parameter	Description
vrf-name	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 Examples The following example binds the interface VLAN 1 to a multiprotocol VRF vrf1.

```
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 Description N/A

7.10 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
vrf-name	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 bind interface to a VRF if it has configed 'vrf receive'
```

Configuration Examples N/A

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.

Platform Description N/A

7.11 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.
vrf-name	(Optional) Name of the VRF

Defaults All VRF information is displayed without parameter specified.

Command mode Privileged EXEC 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 Examples The following example displays the VRF information.

```
Ruijie#show ip vrf
Name                                Interfaces
aaa                                 GigabitEthernet 0/0
                                         GigabitEthernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.12 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** | **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.
detail	Displays the detailed VRF (including the single-protocol VRF and the multiple-protocol) information.
vrf-name	VRF name.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays brief information about all VRF.

```
Ruijie#show vrf
  Name       Default RD        Protocols   Interfaces
  aaa        <not set>         ipv4
  aab        <not set>
  bbb        <not set>         ipv6
  ccc        <not set>         ipv4,ipv6   Vl1
```

:

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 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 Examples The following example clears the RIPng routes:

```
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
metric	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 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 Description N/A

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
distance	Sets the RIPng administrative distance. The range is from 1 to 254.

Defaults 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	N/A

Platform Description N/A

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 *prefix-list-name*	Name of the prefix list which is used to filter the route.
in | **out**	Filters the in or out route in the distribute list.
interface-type interface-name	(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 Description N/A

8.5 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 *metric-value*	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

8.6 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 N/A

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

8.7 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
value	Sets the interface metric value on the interface. The valid range is from 1 to 16.

Defaults 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

8.8 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

8.9 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.
interface-type interface-num	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

8.10 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 [*area-tag*]	Redistributes the ISIS routes to RIPng. *area-tag* indicates the ISIS process number.
ospf *process-id*	Redistributes the OSPF routes to RIPng. *process-id* indicates the OSPF process number, and the range is from 1 to 65,535.
static	Redistributes the static routes to RIPng.
metric *metric-value*	(Optional) Sets the metric value for the route redistributed to RIPng.
route-map *route-map-name*	(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 Description N/A

8.11 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.

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 Description N/A

8.12 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.

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

8.13 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 Description N/A

8.14 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
update	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.
invalid	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.
flush	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 Examples 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.

```
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 Description N/A

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
vrf *vrf_name*	(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.
network	Specifies the route cache of the network or subnet.
netmask	(Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match *network* with the route. The cache of the longest match is cleared.

Command mode Privileged EXEC mode.

Usage guidelines Clearing route cache clears the corresponding routes and triggers the routing protocol relearning. 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 This command is not supported on layer 2 devices.

9.2 ip default-network

Use this command to configure the default network globally. Use the **no** form of this command to restore the default setting.

ip default-network *network*

no ip default-network *network*

Parameter description

Parameter	Description
network	Default network

Default configuration The default is 0.0.0.0/0.

Command mode Global configuration mode.

Usage guidelines
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.
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.

Examples
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.

```
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.

9.3 ip fast-reroute route-map

Use this command to enable static fast reroute. Use the **no** 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*]

Parameter description

Parameter	Description
vrf *vrf-name*	VRF.
route-map *route-map-name*	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

Command	Description
fast-reroute	Configures OSPF fast reroute.

Platform description N/A

9.4 ip route

Use this command to configure a static route. Use the **no** 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]** [**weight** *number*] [**disable** | **enable**]

no ip route [**vrf** *vrf_name*] *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent]** [**weight** *number*] [**disable** | **enable**]

Parameter description

Parameter	Description
vrf-name	Name of the VRF, which can be the single protocol IPv4 VRF or configured IPv4 address family multi-protocol VRF.
network	Network address of the destination
net-mask	Mask of the destination
ip-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The administrative distance of the static route
tag	(Optional) The tag of the static route
permanent	(Optional) Permanent route ID
number	(Optional) Weight number of the static route
disable/enable	(Optional) Disablement or enablement ID of the static route

Default configuration No static route is configured by default.

Command mode Global configuration mode

Usage guidelines

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 flows 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.

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 thought other interface in case of interface failure. The following example configures data flows to be sent through fastehternet 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 This command is not supported on layer 2 devices.

9.5 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*]

Parameter

Parameter	Description

description

vrf *vrf-name*	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
interface-type interface-number	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 *ip-address*	(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.

Default configuration The static address is not correlated with BFD by default.

Command mode Global configuration mode.

Usage guidelines

⚠ 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 This command is not supported on Layer 2 devices.

9.6 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

Parameter description	**Parameter**	**Description**
	N/A	N/A

Default configuration	This function is enabled by default.
Command mode	Global configuration mode.
Usage guidelines	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. `*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	This command is not supported on Layer 2 devices.

9.7 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** form of this command to disable this function.
ip routing
no ip routing

Default configuration	This function is enabled by default.
Command mode	Global configuration mode.
Usage guidelines	IP routing is not necessary when the switch serves as bridge or VoIP gateway.
Examples	The following example disables IP routing. `no ip routing`
Related commands	N/A

Platform description	This command is not supported on Layer 2 devices.

9.8 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** form of this command to restore the default setting.

ip static route-limit *number*

no ip static route-limit *number*

Parameter description	**Parameter**	**Description**
	number	Upper threshold of static routes

Default configuration	The default is 1024.
Command mode	Global configuration mode.
Usage guidelines	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	This command is not supported on Layer 2 devices.

9.9 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** 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*]

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*] [**tag** *tag*] [**weight** *number*]

Parameter description	**Parameter**	**Description**
	network	Network address of the destination
	vrf-name	Name of VRF, which must be the configured IPv6 address family multi-protocol VRF.
	prefix-length	Mask length of the destination

ipv6-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
vrf-name1	VRF the nexthop belongs, which must be the configured IPv6 address family multi-protocol VRF.
distance	(Optional) The administrative distance of the static route. The default is 1.
tag	(Optional) The tag value of the static route. The default is 0.
number	(Optional) The weight value of the static route, which is specified when configuring the equivalent routes, in range of 1 to 128. The sum of the weight of all equivalent paths of one route could not exceed the number of the configurable maximum equivalent paths. The weight ratio between the equivalent routes of the same route shows the flow rate between these paths.

Default configuration

No IPv6 static route is configured by default.

Command mode

Global configuration mode.

Usage guidelines

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.
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.

Examples

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance is 115.

```
ipv6 route 2001::/64 2002::2 115
```

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 fastehternet 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

This command is not supported on Layer 2 devices.

9.10 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 description

Parameter	Description
vrf *vrf-name*	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
interface-type interface-number	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 *ipv6-address*	(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.

Default configuration

The static route is not associated with BFD by default.

Command mode

Global configuration mode.

Usage guidelines

⚠ 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 *2001:1::2*.

```
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	This command is not supported on Layer 2 devices.

9.11 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** form of this command to restore the default setting.

Ipv6 static route-limit *number*

no ipv6 static route-limit *number*

Parameter description

Parameter	Description
number	Upper threshold of static routes in the range from 1 to 10000.

Default configuration	The default is 1000.
Command mode	Global configuration mode.
Usage guidelines	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. `Ruijie# ipv6 static route-limit 900` `Ruijie# no ipv6 static route-limit`

Related commands

Command	Description
ipv6 route	Configures the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table

Platform description	This command is not supported on Layer 2 devices.

9.12 ipv6 unicast-routing

Use this command to enable the IPv6 route function of the RGOS. Use the **no** form of this command to disable this function.

ipv6 unicast-routing

no ipv6 unicast-routing

Parameter description	None
Default configuration	This function is enabled by default.
Command mode	Global configuration mode
Usage guidelines	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

Platform description	This command is not supported on Layer 2 devices.

9.13 maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** form of this command is used to restore the default setting.

maximum-paths *number*

no maximum-paths *number*

Parameter description

Parameter	Description
number	Number of equivalent routes in the range from 1 to 32

Default configuration	The default is 32 for routers. For switches, it depends on switch models.
Command mode	Route map configuration mode.
Usage guidelines	With this command executed, the number of routes for load balancing is no more than the specified number of equivalent routes. You can view the number of equivalent routes with the show running config command.
Examples	The following example sets the number of equivalent routes to 10 and then restores the default setting. `maximum-paths 10`

```
no maximum-paths 10
```

9.14 show ip route

Use the command 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 description

Parameter	Description
vrf *vrf_name*	(Optional) Displays the route information of the VRF.
network	(Optional) Displays the route information to the network.
mask	(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)
protocol	(Optional) Displays the route information of specific protocol.
process-id	(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.

Default configuration

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.

Usage guidelines

This command can display route information flexibly.
This command shows all routes. To show different attributes of routes, specify normal | ecmp | fast-reroute.

Examples

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.
```

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
```

```
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
```

9.15 show ip route static bfd

Use this command to display the IP route correlated BFD information

show ip route [[**vrf** *vrf_name*] **static bfd**

Parameter description	**Parameter**	**Description**
	vrf *vrf-name*	(Optional) Displays route information of the specified VRF. The default is global VRF.
Default configuration	N/A	
Command mode	Privileged EXEC mode.	
Usage guidelines	Use this command to display the IP route correlated BFD information	
Examples	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
```

Field	Description
S	Static route
BFD state	State of the static route correlated BFD.

Related commands N/A

Platform description This command is not supported on Layer 2 devices.

9.16 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 description

Parameter	Description
vrf-name	VRF name

Default configuration 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

VRF1
 Memory: 2000 bytes
    Entries: 22,based on route prefixes
                NORMAL ECMP FRR TOTAL
        Connected 3 0 0 3
```

Examples

9.17 show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

show ipv6 route [vrf *vrf-name***]** [[*network / prefix-length*] | **summary** | *protocol***| weight**]

Parameter description

Parameter	Description
network	(Optional) Displays the route information to the network.
vrf-name	VRF name.
summary	(Optional)Displays the classified statistics of the number of ipv6 routes.
protocol	((Optional) Displays the route information of specific protocol.
weight	(Optional) Displays the non-default-weight routes only.

Default configuration

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.

Usage guidelines

Use this command to display route information flexibly.

Examples

The following example displays the output of this command.

```
Ruijie(config)# show ipv6 route

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 This command is not supported on Layer 2 devices.

9.18 show ip route static bfd

Use this command to display the IPv6 route correlated BFD information

show ipv6 route [[**vrf** *vrf_name*] **static bfd**

Parameter description

Parameter	Description
vrf *vrf-name*	(Optional) Displays the route information of the designated VRF name of the static route. The default is global VRF,

Default configuration N/A

Command mode Privileged EXEC mode.

Usage guidelines Use this command to display the IPv6 route correlated BFD information.

Examples

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
```

Field	Description
S	Static route
BFD state	State of the static route associated BFD

Related commands N/A

Platform description This command is not supported on Layer 2 devices.

9.19 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

Parameter	Description
vrf-name	(Optional) VRF name. If no VRF name is specified, statistics of the IPv6 routing table of the global VRF are displayed. .

Default configuration N/A

Command mode Privileged EXEC mode.

Usage guidelines N/A

Examples

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
```

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 summary.

Related commands

Command	Description
N/A	N/A

Platform description This command is not supported on Layer 2 devices.

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
start-time	Start time of the lifetime. The syntax is as follows: *hh:mm:ss month date year* *hh:mm:ss date month year* ● 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.
end-time	*End time of the encryption key. It must be later than the start time.*
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	Command	Description
	-	-

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
	path-list-num	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.
	regular-expression	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 community list and control access to it. Use the **no** form of this command to remove the setting.

ip community-list {[**standard | expanded**] *community-list-name* | *community-number* } {**permit** | **deny**} [*community-number*]

no ip community-list {**standard | expanded**} {*community-list-name* | *community-number*}

Parameter description

Parameter	Description
community-list-name	Name of the community list of no more than 32 characters
standard	Set a standard community list numbered in 1 to 99.
expanded	Set an expanded community list numbered over 100.
permit	Permit access to the community list.
deny	Deny access to the community list.
community-number	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: Internet: Indicates the Internet community. All paths belong to this community. no-export: Indicates that this path will not be advertised to any EBGP peers. no-advertise: Indicates that this path will not be advertised to any BGP peers. 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.

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 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
prefix-list-name	Name of the prefix list
seq-number	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.
ip-prefix	Network address and mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
maximum-prefix-length	(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
```

10.5 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
prefix-list-name	Name of the prefix list
description-text	Description of the prefix list

Default configuration

No description is added for a prefix list, by default.

Command mode

Global configuration mode

Examples

The example below adds the description for the prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description Deny routes from Net-A
```

10.6 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

Examples

The example below adds a sequence number for the prefix list:

```
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

10.7 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 description

Parameter	Description
prefix-list-name	Name of the prefix list
seq-number	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.
ipv6-prefix	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
maximum-prefix-length	(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

Usage guideline The ipv6 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 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

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 2222::/64.

```
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
```

10.8 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 description

Parameter	Description
prefix-lis-name	Name of the ipv6 prefix list
description-text	Description of the ipv6 prefix list

Default configuration

No description is added for an IPv6 prefix list, by default.

Command mode

Global configuration mode

Examples

The example below adds the description for the prefix list:

```
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.

10.9 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
Examples	The example below adds a sequence number for the prefix list: `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 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 description

Parameter	Description
key-id	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 -

10.11 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 description	Parameter	Description
	key-chain-name	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 -

10.12 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.
text	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 -

10.13 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
as-path-acl-list-num	ACL number, in the range of 1 to 500.
access-list-name	Name of the access list

Default configuration None.

Command mode Route map configuration mode.

Usage guidelines

The match as-path can be followed by an access list number or name.
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

```
!
route-map ROUTEMAP2IBGP
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.

10.14 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
community-list-number	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
community-list-name	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.

Usage guidelines

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.
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

```
ip community-list 1 permit 100:2 100:30
route-map set lopref
match community 1 exact-match
set local-preference 20
```

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 metric-type	Set the metric type.

10.15 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 description

Parameter	Description
standard-list-number	Standard extcommunity list number, ranging from 1 to 99. An extcommunity list may contains multiple excommunity values.
standard-list-name	Standard excommunity name. An extcommunity list may contains multiple excommunity values.
expanded-list-num	Expanded extcommunity list number, ranging from 100 to 199. An extcommunity list may contains multiple excommunity values.
expanded-list-name	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 guideline There are the following scenarios for a route map with an extcommunity:

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 -

10.16 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
interface-type	Interface type
interface-number	Interface number

Default configuration None.

Command mode Route map configuration mode.

Usage guidelines

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.

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 redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol.

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.

10.17 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
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

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.
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 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.

Examples

```
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.

10.18 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
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow match ip next-hop.

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.

Examples

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
```

Related

Command	Description

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 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 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	*access-list-number*	Number of the access list
	access-list-name	Name of the access list
	prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

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.

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.

Examples

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.

```
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
```

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 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.

10.20 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
access-list-name	Name of the access list.
prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

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.

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.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list v6acl, with the default metric being 30.

```
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 ipvr 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.

10.21 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

Parameter	Description

description

access-list-name	Name of the IPv6 access list.
prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

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 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.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 40.

```
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.

10.22 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

Parameter	Description
access-list-name	Name of the IPv6 access list.
prefix-list *prefix-list-name*	Specify the IPv6 prefix list to match.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

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.

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.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 50.

```
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.

10.23 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
metric	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.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10.

```
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.

10.24 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 infilter 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 infilter 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 -

10.25 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.

10.26 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** }

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 guideline 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.

Examples

In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain.

```
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.

10.27 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
tag	Route tag

Default configuration None

Command mode Route map configuration mode

Usage guideline

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.
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.

Examples

In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain.

```
router rip
redistribute ospf 100 route-map redrip
network 192.168.12.0

route-map redrip permit 10
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.

10.28 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 -

10.29 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 description

Parameter	Description
route-map-name	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.
sequence-number	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.

Usage guidelines

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.

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.

Examples

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.

```
!
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.

10.30 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
start-time	Start time of the lifetime. The syntax is as follows: *hh:mm:ss month date year* *hh:mm:ss date month year* ● 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.
end-time	*End time of the encryption key. It must be later than the start time.*
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 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 -

10.31 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
as-number	AS number of the aggregator
ip_address	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.

10.32 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
as-number	AS 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 15 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.

10.33 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
community-list-number	Number of the community list. Standard community list number : 1-99. extended community list number : 100-199.
community-list-name	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.

10.34 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

Parameter	Description
community-number	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.

10.35 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

Parameter	Description
half-life	Half dampening life for the reachable or unreachable route in the range of 1 to 45 minutes, 15 minutes by default
reuse	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
suppress	When the route penalty is higher than this value, the route is suppressed. It is in the range 1 to 20000, 2000 by default
max-suppress-time	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.

10.36 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.
extend-community-value	Extended community value.

Default configuration 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
```

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 metric-type	Set the metric type.

10.37 set extcomm-list delete

Use this command to delete all extcommunity values in the extcommunity list that meet the match rules. Use the **no** form of this command to delete the configuration.

set extcomm-list { *extcommunity-list-number* | *extcommunity-list-name* } **delete**

no set extcomm-list { *extcommunity-list-number* | *extcommunity-list-name* } **delete**

Parameter description

Parameter	Description
extcommunity-list-number	*extcommunity-list-number* Standard list: ranges from 1 to 99. Expanded list: ranges from 100 to 199.
extcommunity-list-name	*extcommunity-list-name* It consists of a maximum of 80 characters.

Default -

Command mode Route map configuration mode.

Usage guideline This command is used to delete the **extcommunity-list.**
This command applies only to policy route configuration.

Examples

```
Ruijie(config)# router bgp 65530
Ruijie(config-router)# neighbor 172.16.233.33 remote-as 65531
Ruijie(config-router)# address-family vpnv4 unicast
Ruijie(config-router-af)# neighbor 172.16.233.33 activate
Ruijie(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPIN in
Ruijie(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out
Ruijie(config-router)# exit
Ruijie(config)# ip extcommunity-list 10 permit rt 100:10
Ruijie(config)# ip extcommunity-list 10 permit rt 100:20
Ruijie(config)# ip extcommunity-list 120 deny 100:50
Ruijie(config)# ip extcommunity-list 120 permit 100:.*
Ruijie(config)# route-map ROUTEMAPIN permit 10
Ruijie(config-route-map)# set extcomm-list 10 delete
Ruijie(config-route-map)# exit
```

```
Ruijie(config)# route-map ROUTEMAPOUT permit 10
Ruijie(config-route-map)# set extcomm-list 120 delete
```

Related command

Command	Description
ip extcommunity-list	Configure an **extcommunity-list.**
match as-path	Match the AS_PATH value
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set extcomm-list delete	Set delete **extcommunity-list.**
set local-preference	Set local preference for a reroute.

Platform description

-

10.38 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
interface-type interface-number	Backup outgoing interface.
ip-address	Backup next-hop.

Default

-

Command mode

Route map configuration mode.

Usage guideline

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.

This command is used for fast reroute configuration.

IP FRR backup routes must not be direct-connection or local host routes.

Examples

```
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
```

Related command	Command	Description
	match ip-address	Match IP address list.

Platform description N/A

10.39 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
	ip-address	IP address of the next hop.
	weight	Weight of the next hop.

Default configuration None

Command mode Route map configuration mode

Usage guideline

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.

Note: If a weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In this mode, the weight of those next hop IP addresses whose weight is not configured is 1 by default.

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.

Examples

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.

```
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
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

Platform description

N/A

10.40 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
dscp-value	DSCP value

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 ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

10.41 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
ip-address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration None

Command mode Route map configuration mode

Usage guideline

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.

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
```

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

10.42 set ip next-hop verify-availability

Use this command to verify the availability of the next hop IP address through BFD. Use the **no** form of this command to remove the setting.

set ip next-hop verify-availability *ip-address* **bfd** *interface-type interface-number gateway*

no set ip next-hop verify-availability *ip-address* **bfd** *interface-type interface-number gateway*

Parameter description

Parameter	Description
ip-address	IP address of the next hop
interface-type	Interface type
interface-number	Interface number

gateway	Gateway address.

Default configuration None

Command mode Route map configuration mode

Usage guideline None

Examples N/A

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

10.43 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

Default configuration 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.

Examples

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:

```
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.

10.44 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

Default configuration 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.

Examples 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:

```
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.

10.45 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*] [*…ipv6-address*[*weight*]]

no set ipv6 default next-hop *glocal-ipv6-address* [weight] [*…ipv6-address*[*weight*]]

Parameter description

Parameter	Description
global-ipv6-address	IPv6 address of the next hop. The next hop router must be the neighbor router.
weight	Weight in the load balancing mode, in the range of 1 to 8.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

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.

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

Examples

The following examle 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*

```
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
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

10.46 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 [vrf *vrf-name* **| global]** *global-ipv6-address* [weight] [*…global-ipv6-address* [*weight*]]

no set ip next-hop [vrf *vrf-name* **| global]** *global-ipv6-address* [weight] [*…global-ipv6-address* [*weight*]]

Parameter description

Parameter	Description
global-ipv6-address	IPv6 address of the next hop. The next hop router should be the neighbor router.
vrf *vrf-name*	The nexthop belongs to the specified VRF which must be the configured IPv6 address family multi-protocol VRF.
global	The nexthop belongs to the global.
weight	Weight of the next hop in the load balancing mode, in the range of 1to 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 pubic 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 bellows.
set ipv6 next-hop;
usual route (the non default route)
set ipv6 default next-hop
Default route.

Examples

The following examle 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*

```
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

10.47 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
critical, flash, flash-override, immediate, internet , network , priority , routine	The precedence type of the IPv6 head.
0~7	The configurable precedence range.

Default configuration

N/A

Command mode

Route map configuration mode

Usage guideline

The following table shows the corresponding relationship between the value and type.

Value	Type
0	routing
1	priority
2	network
3	internet
4	immediate
5	flash-override
6	flash
7	critical

Examples

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

```
Ruijie(config-route-map)# set ipv6 precedence immediate
```

Related commands

Command	Description
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 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

10.48 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

Default configuration None

Command mode Route map configuration mode

Examples

In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area.

```
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.

10.49 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
number	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.

10.50 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
metric-value	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

Usage guideline

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attentions 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.

Examples

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
```

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.

10.51 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
type	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

Usage guideline

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.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.

```
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.

10.52 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-learnt and BGP-sent routes with MLPS labels.

Platform description -

10.53 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
	ip-address	IP address of the next hop.

Default configuration None

Command mode Route map configuration mode

Usage guideline

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.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2.

```
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.

10.54 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.

10.55 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 description	**Parameter**	**Description**
	ip-addr	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.

10.56 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 description

Parameter	Description
tag	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.

Examples The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.

```
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.

10.57 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 description

Parameter	Description
number	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.

Examples

The following example sets the weight for the BGP route learned from the neighbor 1.1.1.1 at the inbound direction to 100.

```
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.

10.58 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 description

Parameter	Description
num	AS path access list number.

Default

N/A

Command

Privileged EXEC mode

mode

Usage guideline N/A

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 -

10.59 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
community-list-number	Number of the community list.
community-list-name	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.

10.60 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
extcommunity-list-num	extcommunity-list number, ranging from 1 to 199.
extcommunity-list-name	extcommunity-list name.

Default -

Command mode Privileged EXEC 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 -

10.61 show ip prefix-list

Use **show ip prefix-list** to display the prefix list or the entries.

show ip prefix-list [*prefix-name*]

Parameter description	Parameter	Description
	prefix-name	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
ip prefix-list name : test
seq pre: 2 entries
seq 5 permit 192.168.564.0/24
seq 10 permit 192.2.2.0/24
```

10.62 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 description	Parameter	Description
	prefix-name	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
permit 13::/20
```

10.63 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 description	**Parameter**	**Description**
	vrf-name	VRF name

Default configuration N/A

Command mode Privileged user mode

Usage guideline N/A

Examples

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

VRF1
 Memory: 2000 bytes
    Entries: 22,based on route prefixes
                NORMAL ECMP FRR TOTAL
```

10.64 show key chain

Use this command to display the key chain configuration.

show key chain [*key-chain-name*]

Parameter description

Parameter	Description
key-chain-name	(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# sh key chain
key chain ripkeys
 key 1 -- text "abc"
 accept-lifetime (00:00:00 Sep 09 2000) - (00:00:00 Dec 12 2011)
 send-lifetime (00:00:00 Sep 09 2000) - (00:00:00 Dec 12 2011)
```

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

-

10.65 show route-map

Use the command to display the configuration of the route map.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
route-map-name	(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 Configuration 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

Parameter	Description
*	Removes all the forwarding information in the IP multicast route table.
group-address	Group IP address of IP multicast routes.
source-address	Source IP address of multicast routes.

Command Mode Privileged EXEC mode

Configuration 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
```

Related Commands

Command	Description
show ip mroute	Displays the forwarding information of multicast routes.

Platform Description N/A

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

Parameter	Description
*	Removes all the forwarding entries in the multicast route table.
group-address	Group IP address of IP multicast routes
source-address	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.

Configuration 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	Displays the multicast route forwarding information.
clear ip mroute	Clears the multicast route forwarding information.

Platform Description

N/A

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*] { *rpf-addrress* | *interface-type interface-number* } } [*distance*]

no ip mroute *source-address mask* [*protocol*]

default ip mroute *source-address mask* [*protocol*]

Parameter Description

Parameter	Description
source-address	Source IP address of the multicast route
protocol	(Optional) The unicast routing protocol being used.
rpf-address	Incoming interface of the multicast route
interface-type interface-number	Interface type and interface ID.
distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Defaults

distance: 0.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure the route for the purpose of RFF check. Note that the configured route is prior to the route learned in the unicast form.

Configuration 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
```

Platform Description

N/A

1.4 ip multicast-routing

Use this command to enable multicast routing forwarding.

Use the **no** form of this command to disable multicast routing forwarding.

ip multicast-routing

no ip multicast-routing

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults Disabled.

Command Mode Global configuration mode

Usage Guide This command allows you to enable IPv4 multicast routing forwarding. The multicast protocol will not be enabled with IPv4 multicast routing forwarding disabled.

Configuration Examples This command enables multicast routing forwarding.

```
Ruijie(config)# ip multicast-routing
```

Platform Description N/A

1.5 ip multicast boundary

Use this command to configure the boundary of an IP multicast group.

Use the **no** or **default** form of this command to remove the configured boundary.

ip multicast boundary *access-list* [**in** | **out**]

no ip multicast boundary *access-list* [**in** | **out**]

default ip multicast boundary *access-list* [**in** | **out**]

Parameter Description	**Parameter**	**Description**
	access-list	Access list associated with the multicast boundary.

Defaults 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.

Configuration Examples

The following example configures svi1 as the boundary of all IP 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
```

1.6 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

default ip multicast route-limit

Parameter Description

Parameter	Description
limit	The number of the entries that can be added to the multicast routing table is 1 to 65,536. The default value is 1024.
threshold	(Optional) Number of multicast routes at which alarms will be triggered. The default value is 65,536.

Defaults

The default value of *limit* is 1024.

The default value of *threshold* is 65536.

Command Mode

Global configuration mode

Usage Guide

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.

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 Examples

The following example sets the route limit to 500.

```
Ruijie(config)# ip multicast route-limit 500
```

Platform Description N/A

1.7 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

default ip multicast rpf longest-match

Parameter Description

Parameter	Description
N/A	N/A

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

Configuration Examples The following example configures to select the routing with the longest-match.

```
Ruijie(config)# ip multicast rpf longest-match
```

Platform Description N/A

1.8 ip multicast static

Use this command to enable flow control for multicast packets on the Layer 2 interface. The **no** or **default** 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*

default ip multicast static *source-address group-address interface-type interface-number*

Parameter Description

Parameter	Description
source-address	Source IP address
group-address	IP address of the multicast group
interface-type interface number	Layer 2 interface on which multicast packets are allowed to forward

Default Disabled

Command Mode Global configuration mode

Usage Guide 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.
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.

Configuration Examples The following example configures forwarding multicast flows (192.168.43.4 and 255.1.1.5) through GigabitEthernet 2/6 and FastEthernet 3/2.

```
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
```

Platform Description This command is supported by switches only.

1.9 ip multicast ttl-threshold

Use this command to configure TTL (time-to-live) threshold on the interface. Use the **no** or **default** form of the command to restore it to the default value.

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

default ip multicast ttl-threshold

Parameter Description

Parameter	Description
ttl-value	TTL threshold on the interface, within the range of 0 to 255.

Default The default *ttl-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.

Configuration Examples

The following example sets the TTL threshold on the interface to 5.

```
Ruijie(config-if)# ip multicast ttl-threshold 5
```

1.10 msf ipmc-overflow override

Use this command to enable the overflow overriding mechanism.

msf ipmc-overflow override

no msf ipmc-overflow override

default msf ipmc-overflow override

Parameter Description

Parameter	Description
N/A	N/A

Default

Disabled.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the overflow overriding mechanism.

```
Ruijie (config)# msf ipmc-overflow override
Ruijie (config)#
```

Platform Description

N/A

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**}

default msf nsf {**convergence-time** | **leak**}

Parameter Description

Parameter	Description
convergence-time *ttl-value*	Maximum time for the multicast protocol convergence, in the valid range of the 0 to 3,600 seconds.

leak *interval*	Packet multicast leak time, in the valid range of 0-3,600 seconds.

Default

convergence-time *time* : 20 seconds;
leak interval: 30 seconds

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum time for the protocol convergence.

```
Ruijie (config)# msf nsf convergence-time 300
Ruijie (config)#
```

The following example sets the packets leak time:

```
Ruijie(config)# msf nsf leak 200
Ruijie(config)#
```

Platform Description

N/A

1.12 show ip mrf mfc

Use this command to display the IPv4 multicast routing forwarding table.

show ip mrf mfc [*source-address group-address*]

Parameter Description

Parameter	Description
source-address	Source address of the multicast routing forwarding entries.
group-address	Group address of the multicast routing forwarding entries.

Defaults

All IPv4 multicast routing forwarding entries are displayed by default.

Command Mode

Privileged EXEC mode

Usage Guide

The three parameters in this command are optional, wherein the source address and group address must be specified at the same time.

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.

Configuration Examples

The following example displays 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)
```

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.
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.

Platform Description N/A

1.13 show ip mroute

Use this command to display the multicast forwarding table.

show ip mroute [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]

Parameter Description

Parameter	Description
group-address	Multicast group IP address
group-or-source-address	Multicast or source IP address. The two addresses must not be the multicast addresses or source addresses at the same 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\Global configuration mode\Interface configuration mode

Configuration Examples

The following example displays 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 displays 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 displays 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 recv 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 recv/Reg NACK recv/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 recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
```

```
Reg pkt counts: Reg ACK recv/Reg NACK recv/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 displays 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.

Platform Description N/A

1.14 show ip mroute static

Use this command to display the v4 static multicast routing information.

show ip mroute static

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode\Global configuration mode\Interface configuration mode

Usage Guide Use this command to display the user-configured static multicast routing. In the same conditions, the priority of the static multicast routing is higher than the dynamically learned.

Configuration Examples

The following example displays the information of the user-configured static multicast routing:

```
Ruijie#show ip mroute static
Mroute: 172.16.0.0, RPF neighbor: 172.30.10.13
 Protocol: , distance: 0
```

The following example displays the information of the user-configured static multicast routing:

```
Ruijie# show ip mroute static
Mroute: 172.16.0.0, distance: 0
```

Platform Description N/A

1.15 show ip mvif

Use this command to display the basic information of the multicast interface.

show ip mvif { *interface-type interface-number* }

Parameter Description	Parameter	Description
	interface-type interface-number	Interface Type and number

Command Mode Privileged EXEC mode\Global configuration mode\Interface configuration mode

Configuration Examples

The following example displays the basic information of the multicast interface of svil.

```
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
```

Platform Description N/A

1.16 show ip rpf

Use this command to display the RPF information of the specified source IP address.

show ip rpf {*source-address* [*group-address*] [**rd** *route-distinguisher*]} [**metric**]

Parameter Description

Parameter	Description
source-address	Specified source IP address
group-address	Specified source IP address
rd *route-disting unisher*	Use the RD proxy for the searching.
metric	Show the metric of the MDT-SAFI route.

Command Mode Privileged EXEC mode\Global configuration mode\Interface configuration mode

Configuration Examples

The following example displays the information of the RPF to 192.168.1.54:

```
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
```

Platform Description N/A

1.17 show msf msc

Use this command to display IPv4 multi-layer multicast forwarding table.

show msf msc [*soured-address*] [*group-address*] [*vlan-id*]

Parameter Description

Parameter	Description
source-address	Specified source IP address of the multi-layer multicast forwarding table.
group-address	Specified group address of the multi-layer multicast forwarding table.
vlan-id	The Vlan id where the incoming interface of the multi-layer multicast forwarding table is. 4096 indicates a routed port.

Defaults All IPv4 multi-layer multicast forwarding entries are displayed by default.

Command Mode Privileged EXEC mode\Global configuration mode\Interface configuration mode

Usage Guide

The three parameters in this command are optional.
If no source address and group address are specified, all mfc entries are displayed.

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.

Configuration Examples

The following example displays 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.

Platform Description N/A

1.18 show msf nsf

Use this command to display the configuration of continuous multicast forwarding.

show msf nsf

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode\Global configuration mode\Interface configuration mode

Configuration Examples

The following example displays 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	Configures the multicast NSF parameter.

Platform N/A

Description

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

Parameter	Description
*	Removes all the forwarding information in the IPv6 multicast route table.
v6group-address	Group IPv6 address of IPv6 multicast routes.
v6source-address	Source IPv6 address of multicast routes.

Command Mode Privileged EXEC mode

Configuration Examples The following example removes all the multicast routing entries.

```
Ruijie# clear ip mroute *
```

Related Commands

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

Parameter	Description
*	Removes all the forwarding entries in the multicast route table.
v6group-address	Group IPv6 address of IPv6 multicast routes
v6source-address	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 Examples The following example clears all the statistical information of the multicast routing entries.

```
Ruijie# clear ip mroute statistics *
```

Related Commands

Command	Description
show ipv6 mroute	Displays the multicast route forwarding information.

clear ipv6 mroute	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-addrress* | *interface-type interface-number*} [*distance*]

no ipv6 mroute *ipv6-prefix/prefix-length* [*protocol as-number*] { *v6rpf-addrress* | *interface-type interface-number*} [*distance*]

Parameter Description

Parameter	Description
ipv6-prefix/prefix-length	Source IPv6 address of the multicast route.
protocol	(Optional) The unicast routing protocol being used.
v6rpf-address	Incoming interface of the multicast route
interface-type interface-number	Interface type and interface ID.
distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.

Default The static IPv6 multicast routing is not configured by default.

Command Mode Global configuration mode

Usage Guide

This command is used to configure the route for the purpose of RFF 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.

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 Description

Parameter	Description
access-list-name	Access list associated with the multicast boundary.

Default The boundary of a specified IPv6 multicast group is not 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 IPv6 address.

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.

Configuration Examples

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
```

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

Parameter	Description
limit	The number of the entries that can be added to the IPv6 multicast routing table is 1 to 65,536.
threshold	(Optional) Number of IPv6 multicast routes at which alarms will be triggered.

Default

The default value of *limit* is 1,024.

The default value of *threshold* is 65,536.

Command Mode Global configuration mode

Usage Guide

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.

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 Examples The following example sets the route limit to 500 and the warning value 90.

```
Ruijie(config)# ipv6 multicast route-limit 500 90
```

2.6 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 Description

Parameter	Description
N/A	N/A

Default This function is disabled by default

Command Mode Global configuration mode

Usage Guide

Use this command to enable the IPv6 multicast routing forwarding. With this function disabled, the multicast protocol cannot be enabled.

This command must be configured to enable the IPv6 multicast routing forwarding. This function conflicts with IGMP Snooping.

Configuration Examples The following example enables the IPv6 multicast routing forwarding.

```
Ruijie(config)# ipv6 multicast-routing
```

2.7 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 Description	**Parameter**	**Description**
	N/A	N/A

Default	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, 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`

2.8 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	**Parameter**	**Description**
	source-address	Source IPv6 address
	group-address	IPv6 address of the multicast group
	interface-type interface number	Layer 2 interface on which multicast packets are allowed to forward

Default	This function is disabled by default.
Command Mode	Global configuration mode

Usage Guide

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.

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
```

2.9 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 Description

Parameter	Description
convergence-time *time*	Maximum duration for which the system waits for multicast protocol convergence. The unit is second. The value ranges from 0 to 3600.
leak *interval*	Interval at which multicast packets are leaked. The unit is second. The value ranges from 0 to 3600.

Default

The default convergence-time is 20 and leak interval is 30.

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
```

Platform Description

N/A

2.10 show ipv6 mroute

Use this command to display the IPv6 multicast forwarding table.

show ipv6 mroute [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]

Parameter Description

Parameter	Description
v6group-address	Multicast group IPv6 address
v6source-address	Multicast source IPv6 address
summary	Displays the summary of the multicast routing table.
count	Displays the count of the multicast routing table.

Command Mode

Privileged EXEC mode

Configuration Examples

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
```

2.11 show ipv6 mroute static

Use this command to display the static IPv6 multicast routing information.

show ipv6 mroute static

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the statically-configured multicast route. Under the same condition, the static multicast route is prior to the unicast route.

Configuration Examples The following example displays the static IPv6 multicast routing information.

```
Ruijie#show ipv6 mroute static
Mroute: 2233::/64, RPF neighbor: 3333::3333
Protocol: , distance: 0
```

2.12 show ipv6 mvif

Use this command to display the basic information of the multicast interface.

show ipv6 mvif { *interface-type interface-number* }

Parameter Description	**Parameter**	**Description**
	interface-type interface-number	Interface Type and number

Command Mode Privileged EXEC mode

Configuration Examples

The following example displays the basic information of the multicast interface of svil.

```
Ruijie#show ipv6 mvif
Interface    Mif Owner    Uptime
      Idx Module
Register     0     03d03h09m
VLAN 1     1  PIMSMV6   03d03h09m
```

2.13 show ipv6 rpf

Use this command to display the RPF information of the specified source IPv6 address.

show ipv6 rpf {*v6source-address*}

Parameter Description

Parameter	Description
v6source-address	Specified source IPv6 address

Command Mode Privileged EXEC mode

Configuration Examples

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
```

2.14 show ipv6 mrf6 mfc

Use this command to display the IPv6 multicast forwarding table.

show ipv6 mrf6 mfc [*v6soure-address v6group-address*]

Parameter Description

Parameter	Description
v6group-address	IPv6 address of a multicast group.
v6source-address	IPv6 address of a multicast source.

Default N/A

Command Mode Privileged EXEC 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 layer-3 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 layer-3 outbound interface of the entries is VLAN 3. 1 indicates the ttl threshold of the layer-3 interface.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.15 show msf6 msc

Use this command to display entries of the IPv6 routing multicast data stream exchange table.

show msf6 msc [*v6soure-address*] [*v6group-address*] [*vlan-id*]

Parameter Description

Parameter	Description
v6group-address	IPv6 address of a multicast group.
v6source-address	IPv6 address of a multicast source.
vlan-id	VLAN ID of the inbound interface of the entries. If the value is greater than 4096, the interface is a routing interface.

Default N/A

Command Mode Privileged EXEC 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 layer-3 interfaces of the entries.
VLAN	Indicates a layer-3 outbound interface VLAN xxx (yyy). If the layer-3 interface is an SVI

4094(8190)	interface, the value of xxx is the VLAN vid of the SVI, and the value of yyy is the VLAN vid+4096. If the layer-3 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 layer-3 interfaces.
1 OPORTs	Number of layer-2 interfaces owned by this layer-3 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 layer-2 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 layer-3 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 Commands

Command	Description
N/A	N/A

Platform Description This command is supported on only switches.

2.16 show msf6 nsf

Use this command to display the multicast non-stop forwarding configuration.

show msf6 nsf

Parameter Description

Parameter	Description
N/A	N/A

Default N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the multicast non-stop forwarding configuration.

```
Ruijie# show msf6 nsf
Multicast HA Parameters
-----------------------------------------------+---------+
protocol convergence timeout    120 secs
flow leak interval      20 secs
```

Related Commands

Command	Description
msf6 nsf	Multicast non-stop forwarding.

Platform Description

This command is supported on only switches.

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
N/A	Deletes all group information.
group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
interface-type	Interface type.
interface-number	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 Examples The following example clears all group entries:

```
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 *ifname*

Parameter Description

Parameter	Description
ifname	Name of the interface

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.

Configuration Examples The following example clears the IGMP entry for the interface.

```
Ruijie# clear ip igmp interface gigabitEthernet 4/1
```

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** form of this command to restore the default setting.

ip igmp access-group *access-list*

no ip igmp access-group

Parameter Description

Parameter	Description
access-list	Name of access control list in the range from 1 to 199, 1300 to 2699, 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 chek. 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 Examples The following example adds the interface Ethernet 0/1 to the group 225.2.2.2.

```
Ruijie# configure terminal
Ruijie(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ip igmp access-group 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)# ip igmp access-group ext_acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.4 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** form of this command to restore the default setting.

ip igmp immediate-leave group-list *access-list*

no ip igmp immediate-leave group-list

Parameter Description

Parameter	Description
access-list	Name of access control list.

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)# ip igmp immediate-leave group-list 1
Ruijie(config-if)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 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** form of this command to restore the default setting.
ip igmp join-group *group-address*
no ip igmp join-group *group-address*

Parameter Description

Parameter	Description
group-address	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 Examples The following example adds a host group member manually.

```
Ruijie# configure terminal
Ruijie(config)# interface fast 0/1
Ruijie(config-if)# ip igmp join-group 233.3.3.3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 ip igmp last-member-query-count

last-member-query-count means the number of query packets that the multicast device will send continuously upon receiving the leave message. Use this command to configure the value of **last-member-query-count**. Use the **no** form of this command to restore the default setting.
ip igmp last-member-query-count *number*
no ip igmp last-member-query-count

Parameter Description

Parameter	Description
number	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 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.

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)# ip igmp last-member-query-count 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 ip igmp last-member-query-interval

Use this command to set the time interval of sending the group query message. Use the **no** form of this command to restore the default setting.

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval

Parameter Description

Parameter	Description
interval	The interval sending the group query message in the range from1 to 255in the unit of 0.1 second.

Defaults The default is 10.

Command Mode Interface configuration mode

Usage Guide 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.

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)# ip igmp last-member-query-interval 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.8 ip igmp limit

Use this command to globally set the maximum number of IGMP group records. Use the **no** form of this command to restore the default setting.

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit

Parameter Description

Parameter	Description
number	Maximum number of IGMP states, depending on devices
except	(Optional) Prevents the groups of the access list from taking part in calculation.
access-list	(Optional) Access list name

Defaults The default is 65536.

Command Mode Global configuration mode/ Interface configuration mode

Usage Guide Use this command to globally configure the maximum number of IGMP group records. The messages of the members exceeding the threshold will not be saved in the IGMP buffer and will not be forwarded.
This command can be configured globally or on the interface The messages of the members will be ignored if they exceed the interface or global configuration.

Configuration Examples The following example sets the maximum number to 300.

```
Ruijie(config) # ip igmp limit 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.9 ip igmp mroute-proxy

Use this command to configure an interface as a mroute-proxy interface that can transmit messages to its uplink ports. Use the **no** form of this command to restore the default setting.
ip igmp mroute-proxy *interfname*
no ip igmp mroute-proxy

Parameter Description

Parameter	Description
interfname	Name of the relevant uplink interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide After an uplink interface is configured as **proxy-service** interface, the interface can forward the IGMP messages sent by other members.

Configuration Examples The following example configures an interface to **mroute-proxy** interface.

```
Ruijie(config-if)# ip igmp mroute-proxy fa 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 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** form of this command to restore the default setting.

ip igmp proxy-service

no ip igmp proxy-service

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide 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 **switchport** 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 Examples The following example configures an interface to the **proxy-service** module.

```
Ruijie(config-if)# ip igmp proxy-service
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.11 ip igmp query-interval

Use this command to configure the query interval of an ordinary member. Use the **no** form of this command to restore the default setting.

ip igmp query-interval *seconds*

no ip igmp query-interval

Parameter Description

Parameter	Description
seconds	Query interval of ordinary member, in the range is from 1 to 18000 in the unit of seconds.

Defaults The default is 125.

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 Examples The following example configures the query interval of ordinary member to 120 seconds on the interface Ethernet 0.

```
Ruijie(config-if)# ip igmp query-interval 120
```

The following example configures the query interval of ordinary member to the default value on the interface Ethernet 0.

```
Ruijie(config-if)# no ip igmp query-interval
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.12 ip igmp query-max-response-time

Use this command to configure the maximum response interval. Use the **no** form of this command to restore the default setting.

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Parameter Description

Parameter	Description
seconds	The maximum response interval, in the range from 1 to 25 seconds.

Defaults The default is 10.

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 20s on the interface Ethernet 0.

```
Ruijie(config-if)# ip igmp query-max-response-time 20
```

The following example configures the maximum response interval to the default value on the interface Ethernet 0.

```
Ruijie(config-if)# no ip igmp query-max-response-time
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.13 ip igmp query-timeout

Use this command to configure the time the device waits before it takes over as the querier. Use the **no** form of this command to restore the default setting.

ip igmp query-timeout *seconds*

no ip igmp query-timeout

Parameter Description

Parameter	Description
seconds	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.

Command Mode Interface configuration mode

Usage Guide IGMPv2 should be run for this command to work. By default, Cisco sets the waiting time of the device to two times of the query interval of **ip igmp query-interval**. In Ruijie, the default value is set to 255s. 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 200s on the interface Ethernet 0/1.

```
Ruijie(config-if)# ip igmp query-timeout 200
```

The following example configures the time the device waits before it takes over as the querier to the default value on the interface Ethernet 0/1.

```
Ruijie(config-if)# no ip igmp query-timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.14 ip igmp robustness-variable

Use this command to change the value of the robustness variable. Use the **no** form of this command to restore the default setting.

ip igmp robustness-variable *number*

no ip igmp robustness-variable

Parameter Description

Parameter	Description
number	The value of robustness variable, in the range from2 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# configure terminal
```

```
Ruijie(config)# interface ethernet 0
Ruijie(config-if)# ip igmp robustness-variable 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.15 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

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.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.16 ip igmp ssm-map static

Use this command to map the static **ssm-map** source IP address to the group records in the global

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

ip igmp ssm-map static *access-list a.b.c.d*

no ip igmp ssm-map static *access-list a.b.c.d*

Parameter Description

Parameter	Description
access-list	ACL name in the range 1 to 99, 1300 to 1999 or characters.
a.b.c.d	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** 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 static 11 192.168.2.2.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.17 ip igmp static-group

Use this command to directly add an interface to a group. You can use this command to add an interface to a group. Use the **no** form of this command to restore the default setting.

ip igmp static-group *group-address*

no ip igmp static-group *group-address*

Parameter Description

Parameter	Description
group-address	Multicast group IP address.

Defaults The switch is not added to the 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.

Configuration Examples The following example adds a host group member manually.

```
Ruijie# configure terminal
Ruijie(config)# interface fast 0/1
Ruijie(config-if)# ip igmp static-group 233.3.3.3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.18 ip igmp version

Use this command to set the version number of IGMP to be used on the interface. Use the **no** form of this command to restore the default setting.
ip igmp version { **1** | **2** | **3** }
no ip igmp version

Parameter Description

Parameter	Description
{ **1** | **2** | **3** }	Three version numbers, in the range from 1 to 3.

Defaults The default is 2.

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 Examples The following example sets the version number to 2.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0
Ruijie(config-if)# ip igmp version 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.19 ip igmp enforce-router-alter

Use this command to receive IGMP report packets with the option of router-alter.
ip igmp enforce-router-alter

Use the **no** form of this command to receive all IGMP report packets.
no ip igmp enfore-router-alter

Use the **default** form of this command to restore the default setting.
default ip igmp enfore-router-alter

Parameter Description

Parameter	Description
N/A	N/A

Defaults All IGMP report packets are received by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example receives IGMP report packets with the option of router-alter..

```
Ruijie# configure terminal
Ruijie(config)#ip igmp enforce-router-alter
```

Platform Description N/A

3.20 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	NA

Defaults The source IP address is not checked by default.

Command Mode Global configuration mode

Usage Guide N/A

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 Description N/A

3.21 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 [**vrf** *vrf-name*] **send-router-alert**
no ip igmp [**vrf** *vrf-name*] **send -router-alert**
default ip igmp [**vrf** *vrf-name*] **send -router-alert**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

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

3.22 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 [*group-address* | *interface-type* | *interface-number*] [**detail**]

Parameter Description

Parameter	Description
group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
interface-type	Interface type.
interface-number	Interface number.
detail	Displays the detailed information.
N/A	Displays the information about all the groups.

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 Description N/A

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
interface-type	Interface type.
interface-number	Interface number.
N/A	Displays information about all the interfaces.

Defaults N/A

Command Mode User EXEC 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.

```
Ruijie# show ip igmp interface
Interface vlan1.1 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying device 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|
IGMP Snooping is globally enabled|
IGMP Snooping is enabled on this interface
IGMP Snooping fast-leave is not enabled
```

```
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 [*A.B.C.D*]

Parameter Description

Parameter	Description
A.B.C.D	Source address to be mapped

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Run this command without any parameter, and all SSM-MAP information is displayed.

Configuration Examples The following example displays the **ssm-map** configuration information.

```
Ruijie# sh ip igmp ssm-mapping
SSM Mapping: Enabled
Database    : Static mappings configured
Show the group information of group 233.3.3.3 to be mapped
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 Description N/A

4. MLD Commands

4.1 clear ipv6 mld group

Use this command to clear the dynamic group member learned by MLD protocol. The dynamic group member refers to the group member record generated by learning the report packets.

clear ipv6 mld group [*group-address*] [*interface-type interface-number*]

Parameter Description

Parameter	Description
group-address	IPv6 multicast group address with 128 bits.
interface-type	The associated interface type.
interface-number	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 Description N/A

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
interface-type	The interface type.
interface-number	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. That packet statistical information include the number of the received report packets, the number of the done packets and 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** form of this command to restore the default setting.

ipv6 mld access-group *access-list*

no ipv6 mld access-group

Parameter Description

Parameter	Description
access-list	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.
TThe multicast group access control command is associated with the extended ACL. When the received MLD report mesage 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)# ipv6 mld access-group acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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** form of this command to restore the default setting.
ipv6 mld immediate-leave group-list *word*
no ipv6 mld immediate-leave group-list

Parameter Description

Parameter	Description
word	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 2s.
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 condion that there is only one host connecting to the interface.

Configuration Examples The following example configures the immediate-leave function.

```
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)# ipv6 mld immediate-leave group-list acl
```

Related Commands

Command	Description
ipv6 mld last-member-query-interval	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** form of this command to restore the default setting.
ipv6 mld join-group *group-address*
no ipv6 mld join-group *group-address*

Parameter Description

Parameter	Description
group-address	The IPv6 non-management multicast group address.

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.
It is worth mentioning that if the group address whose beginning characters are 0xFF*1,0xFF3*, it fails to configure this command. The group address whose beginnning characters are 0xFF*2 fails to form a group.

Configuration Examples The following example adds the host group member:

```
Ruijie# configure terminal
Ruijie(config)# interface fast 0/1
Ruijie(config-if)# ipv6 mld join-group ff55::100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.6 ipv6 mld last-member-query-count

Use this command to set the last-member-query-count number. Use the **no** form of this command to restore the default setting.

ipv6 mld last-member-query-count *number*

no ipv6 mld last-member-query-count

Parameter Description

Parameter	Description
number	The last member query count number. The valid range is 2-7.

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 Examples The following example sets the last-member-query-count number to 3.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# 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** form of this command to restore the default setting.

ipv6 mld last-member-query-interval *interval*

no ipv6 mld ast-member-query-interval

Parameter Description

Parameter	Description
interval	The valid range is 1-255 in the unit of 0.1 seconds.

Defaults The default is 10.

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 fa 0/1
Ruijie(config-if)# ipv6 mld last-member-query-interval 20
```

Related Commands

Command	Description
ipv6 mld immediate-leave	N/A

Platform Description N/A

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** form of this command to restore the default setting.

ipv6 mld limit *number* [**except** *access-list*]

no ipv6 mld limit

Parameter

Parameter	Description

Description

number	The maximum number of the group member learned by the MLD. The valid range is 1-65536.
except *access-list*	(Optional) The ACL beyond the configured mld limit.

Defaults The default is 1024.

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 300.

```
Ruijie(config-if)# ipv6 mld limit 300
```

The following example sets the mld limit to 300, but the configured acl can still learn.

```
Ruijie(config-if)# ipv6 mld limit 300 except acl
```

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** form of this command to restore the default setting.
ipv6 mld mroute-proxy *interface-type interface-number*
no ipv6 mld mroute-proxy

Parameter Description

Parameter	Description
interface-type interface-number	The correspondent connected interface.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide After the connected interface has been configured as the proxy-service interface, it can forward the MLD packets sent from other members

Configuration Examples The following example sets the interface as the mroute-proxy interface.

```
Ruijie(config-if)# ipv6 mld mroute-proxy fa 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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** form of this command to disable the default setting.

ipv6 mld proxy-service

no ipv6 mld proxy-service

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide 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 Examples The following example sets the interface proxy-service.

```
Ruijie(config-if)# ipv6 mld proxy-service
```

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** form of this command to restore the default setting.

ipv6 mld querier-timeout *seconds*

no ipv6 mld querier-timeout

Parameter Description

Parameter	Description
seconds	The querier alive period, in the range from 60 to 300 in the unit of seconds.

Defaults The default is 255.

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** form of this command to restore the default setting.

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

Parameter Description

Parameter	Description
seconds	The query interval for the general member, in the range from 1 to 18000 in the unit of seconds

Defaults The default is 125.

Command Mode Interface configuration 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 Examples The following example sets the query-interval for the general member on the interface Ethernet 0.

```
Ruijie(config-if)# ipv6 mld query-interval 120
```

The following example sets the query-interval for the general member to the default value on the interface Ethernet 0.

```
Ruijie(config-if)# no ipv6 mld query-interval
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.13 ipv6 mld query-max-response-time

Use this command to set the maximum response time. Use the **no** form of this command to restore the default setting.

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

Parameter Description

Parameter	Description
seconds	The maximum response time, in the range from 1 to 25 in the unit of

	seconds

Defaults The default is 10.

Command Mode Interface configuration 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 Examples The following example sets the maximum query response time on the interface gigabitEthernet 0/1.

```
Ruijie(config-if)# ipv6 mld query-max-response-time 20
```

The following example sets the maximum query response time on the interface gigabitEthernet 0/1.

```
Ruijie(config-if)# no ipv6 mld query-max-response-time
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.14 ipv6 mld robustness-variable

Use this command to set querier robustness value. Use the **no** form of this command to restore the default setting.

ipv6 mld robustness-variable *number*

no ipv6 mld robustness-variable

Parameter Description

Parameter	Description
number	Sets the querier robustness value, 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 querier robustness value to 3:

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0
```

```
Ruijie(config-if)# ipv6 mld robustness-variable 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.15 ipv6 mld ssm-map enable

Use this command to enable the mld ssm-map function. Use the **no** form of this command to restore the default setting.

ipv6 mld ssm-map enable

no ipv6 mld 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 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
```

Related Commands

Command	Description
N/A	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 form of this command to restore the default setting.

ipv6 mld ssm-map static *access-list X:X:X:X::X*

no ipv6 mld ssm-map static *access-list X:X:X:X::X*

Parameter Description

Parameter	Description
access-list	Sets the IPv6 ACL name.
X:X:X:X::X	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 Examples The following example maps all group record of the ACL name to the source address 4444::1234.

```
Ruijie(config)# ipv6 mld ssm-map static te 4444::1234
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.17 ipv6 mld static-group

Use this command to add an interface to a group statically. Use the **no** form of this command to restore the default setting.

ipv6 mld static-group *group-address*

no ipv6 mld static-group *group-address*

Parameter Description

Parameter	Description
group-address	Sets the IPv6 non-management multicast group address.

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 Examples The following example adds interface Eth0/1 to group ff55::3 statically.

```
Ruijie# configure terminal
Ruijie(config)# interface fast 0/1
Ruijie(config-if)# ipv6 mld static-group ff55::3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.18 ipv6 mld version

Use this command to set the MLD version number on the interface. Use the **no** form of this command to restore the default setting.

ipv6 mld version { **1** | **2** }

no ipv6 mld version

Parameter Description

Parameter	Description
{ **1** | **2** }	Sets the MLD version number.

Defaults The default is 2.

Command Mode Interface configuration mode

Usage Guide Use this command to control the MLD version number.

Configuration Examples The following example sets the MLD version 1.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ipv6 mld version 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
group-address	Sets the IPv6 multicast group address in 128 bits.
interface-type	Sets the interface type.
interface-number	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 Examples The following example displays all group information.

```
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
interface-type	Sets the interface type.
interface-number	Sets the interface number.

Defaults N/A

Command Mode User EXEC mode / Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the state information of all interfaces.

```
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 Description N/A

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
group-address	Displays the group address.

Defaults N/A

Command Mode User EXEC mode / the Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the state information of all interfaces.

```
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 Examples The following example clears the statistics of PIM-DM packets.

```
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 Description N/A

5.2 ip pim dense-mode

Use this command to enable PIM-DM on the interface. Use the **no** form of this command to restore the default setting.

ip pim dense-mode

no 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.

Configuration Examples The following example enables PIM-DM on the interface.

```
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 neighbor-filter

Use this command to enable the neighbor filtering on the interface. 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. Use the **no** form of this command is to restore the default setting.

ip pim neighbor-filter *access-list*
no ip pim neighbor-filter *access-list*

Parameter Description

Parameter	Description
access-list	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 N/A

Configuration Examples The following example enables the neighbor filtering on the interface.

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim neighbor-filter 14
```

1. 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.

2. 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

5.4 ip pim override-interval

Use this command to reconfigure the override-interval of the hello message. Use the **no** form of this command to restore the default setting.

ip pim override-interval *interval-milliseconds*

no ip pim override-interval

Parameter Description

Parameter	Description
interval-milliseconds	In the range from 1 to 65,535 in the unit of milliseconds.

Defaults The default is 2,500.

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 300 milliseconds.

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim override-interval 3000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.5 ip pim propagation-delay

Use this command to reconfigure the propagation-interval of the hello message. Use the **no** form of this command to restore the default setting.

ip pim propagation-delay *interval-milliseconds*

no ip pim propagation-delay

Parameter Description

Parameter	Description
interval-milliseconds	Propagation-interval of the hello message in the range from 1 to 32,767 in the unit of milliseconds.

Defaults The default is 500.

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 Description N/A

5.6 ip pim query-interval

Use this command to reconfigure the interval of sending the hello message. Use the **no** form of this command to restore the default setting.

ip pim query-interval *interval-seconds*

no ip pim query-interval

Parameter Description

Parameter	Description
Interval-seconds	Interval of sending 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 If **hello interval** is set, the **hello holdtime** value will be updated to 3.5 times of **hello interval**.

Configuration Examples The following example sets the interval of sending the hello message to 123 seconds.

```
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

5.7 ip pim state-refresh disable

Use this command to prohibit the interface from processing and forwarding the PIM-DM state refresh messages. The **no** form of this command to restore the default setting.

ip pim state-refresh disable

no 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 Examples The following example disables the processing of the PIM-DM state refresh message.

```
Ruijie# configure terminal
Ruijie(config)# ip pim state-refresh disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.8 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** form of this command to restore the default setting.
ip pim state-refresh origination-interval *interval-seconds*
no ip pim state-refresh origination-interval

Parameter Description

Parameter	Description
Interval-seconds	Interval of sending the PIM-DM update message in the range from 1 to 100 in unit of seconds.

Defaults The default is 60.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the interval of sending the PIM-DM state refresh message to 65 seconds.

```
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 Description N/A

5.9 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** 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

5.10 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
interface-type interface-number	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 neighbor	Displays the information about the neighbors of the PIM-DM interface.

Platform Description N/A

5.11 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
group-or-source-address	Group address or source address
group-or-source-address	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 Examples The following example displays the information about the PIM-Dm routing table.

```
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 Description N/A

5.12 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

Parameter	Description

Description

interface-type *interface-number*	Interface type and 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 information about the PIM-DM neighbors.

```
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

5.13 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	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 information about the PIM-Dm next hop:

```
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	N/A

Platform Description N/A

5.14 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	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 Examples The following example displays the statistics of the PIM-DM packets.

```
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
*	Clears all RP-SET.

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** form this command to restore the default setting.

ip pim accept-bsr list *access-list*

no ip pim accept-bsr

Parameter Description

Parameter	Description
list *access-list*	IP standard number ACL

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# configure terminal
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-with-null-group

Use this command to receive the C-RP-ADV packets whose prefix-count is 0. Use the **no** form of this command to restore the default setting.

ip pim accept-crp-with-null-group

no 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)# configure terminal
Ruijie (config)# ip pim accept-crp-with-null-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.5 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** form of this command to restore the default setting,

ip pim accept-crp list *access-list*

no ip pim accept-crp

Parameter Description

Parameter	Description
list access-list	IP extension number ACL

Defaults By default, the elected BSR receives all external advertisements of candidate RPs

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 Examples The following example confines the C-RP address range and the multicast group address range it serves.

```
Ruijie (config)# comfigure terminal
Ruijie (config)# ip pim accept-crp list 100
```

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** 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

Parameter Description

Parameter	Description
access-list	Use an extended IP access list to define the (S, G) address range. Access control list supporting numerical ACL in the range of 100 to 199 and 2000 to 2699 and name ACL.
route-map *map-name*	Use 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 Examples The following example confines the source address of register packets on the RP.

```
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	N/A

Platform Description N/A

6.7 ip pim bsr-border

Use this command to configure the BSR border. Use the **no** form of this command to restore the default setting. Use the **no** form of this command to restore the default setting.

ip pim bsr-border

no ip pim bsr-border

Parameter Description	Parameter	Description
	N/A	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 Examples The following example sets the BSR border on the interface *g 0/3*

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ip pim bsr-border
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

6.8 ip pim bsr-candidate

Use this command to configure the C-BSR. Use the **no** 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 [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and number
hash-mask-length	(Optional) HASK mask length configured for electing the RP in the range from 0 to 32. The default is 10.
priority-value	(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 Examples The following example configures the C-BSR.

```
Ruijie# configure terminal
Ruijie(config)# ip pim bsr-candidate g 0/3 30 192
```

Related Commands

Command	Description
access-list	N/A

Platform Description N/A

6.9 ip pim dr-priority

Use this command to set the DR priority, Use the **no** form of this command to restore the default setting.

ip pim dr-priority *priority-value*

no ip pim dr-priority

Parameter Description

Parameter	Description
priority-value	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 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 has 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 Examples The following example sets the DR priority.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ip pim dr-priority 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.10 ip pim ignore-rp-set-priority

Use this command to ignore the RP priority. Use the **no** form of this command to restore the default setting.

ip pim ignore-rp-set-priority

no ip pim ignore-rp-set-priority

Parameter Description

Parameter	Description
N/A	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	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** form of this command to restore the default setting.

ip pim jp-timer *seconds*

no ip pim jp-timer

Parameter Description

Parameter	Description
seconds	Interval to send the join/prune message in the range from 1 to 65535 in the unit of seconds

Defaults The default is 60.

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 50 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip pim jp-timer 50
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.12 ip pim neighbor-filter

Use this command to confine the neighbor address range. Use the **no** form of this command to restore the default setting.

ip pim neighbor-filter *access_list*

no ip pim neighbor-filter *access_list*

Parameter Description

Parameter	Description
access_list	Access control list supporting numerical ACL in the range 1 to 99 and name 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 192.168.1.5.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ip pim neighbor-filter 14
Ruijie(config-if)# exit
Ruijie(config)# access-list 14 deny 192.168.1.5 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description N/A

6.13 ip pim neighbor-tracking

ip pim neighbor-tracking Use this command to disable join restraint on the interface. Use the **no** form of this command to restore the default setting.

ip pim neighbor-tracking

no 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# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# 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** form of this command to restore the default setting.

ip pim override-interval *milliseconds*

no ip pim override-interval

Parameter

Parameter	Description

Description

milliseconds	In the range from 1 to 65535 in the unit of milliseconds

Defaults The default is 2500.

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.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config)# ip pim override-interval 3000
```

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** form of this command to restore the default setting.

ip pim probe-interval *seconds*

no ip pim probe-interval

Parameter Description

Parameter	Description
seconds	In the range from 1 to 65535 seconds

Defaults The default is 5.

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 Examples The following example sets the probe time to 6 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip pim probe-interval 6
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.16 ip pim propagation-delay

Use this command to set the propagation-delay on the interface. Use the **no** form of this command to restore the default setting.

ip pim propagation-delay *milliseconds*

no ip pim propagation-delay

Parameter Description

Parameter	Description
interval-milliseconds	In the range from 1 to 32765 milliseconds

Defaults The default is 500.

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# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config)# ip pim propagation-delay 600
```

Related Commands

Command	Description
ip pim override-interval	N/A
Ip pim neighbor-tracking	N/A

Platform Description N/A

6.17 ip pim query-interval

Use this command to set the interval to send the hello packets. Use the **no** form of this command to restore the default setting.

ip pim query-interval *seconds*

no ip pim query-interval

Parameter Description

Parameter	Description
interval-seconds	Interval to send the Hello message, in the range from 1 to 65535 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 18752.

Configuration Examples The following example sets the interval to send the hello packets to 123 seconds.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config)# ip pim query-interval 123
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.18 ip pim register-checksum-wholepkt

Use this command to calculate the checksum of the whole register packet. Use the **no** 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*]

Parameter Description

Parameter	Description
access-list	Access-list: access control list supporting numerical ACL in the range from100 to 199 and from1300 to 1999 and name ACL. Group-list access-list :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 Examples The following example calculates the checksum of the whole register packet..

```
Ruijie# configure terminal
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 Description N/A

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** form of this command to restore the default setting.

ip pim register-decapsulate-forward

no ip pim register-decapsulate-forward

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 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 decapsulate and forward 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# configure terminal
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

Parameter Description

Parameter	Description
rate	Maximum number of register packets that can be sent per second, in the range from 1 to 65535

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 Examples The following example limits the rate of register packets .

```
Ruijie# configure terminal
Ruijie(config)# ip pim register-rate-limit 3000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.21 ip pim register-rp-reachability

Use this command to check RP reachability before sending register packets**.** Use the **no** form of this command to restore the default setting.

ip pim register-rp-reachability

no 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 Mode Global configuration 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# configure terminal
Ruijie(config)# ipv6 pim register-rp-reachability
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.22 ip pim register-source

Use this command to specify the source IP address of the register packets. Use the **no** form of this command to restore the default setting.

ip pim register-source { *local_address* | *interface-type interface-number* }

no ip pim register-source

Parameter Description

Parameter	Description
interface-type interface-number	Interface whose IP address is used as the source IP address of register packets
local_address	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 Examples The following example specifies the source IP address of the register packets.

```
Ruijie# configure terminal
Ruijie(config)# ip pim register-source 192.168.195.80
Ruijie(config)# ip pim register-source g 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** form of this command to restore the default setting.

ip pim register-suppression *seconds*

no ip pim register-suppression

Parameter Description

Parameter	Description
seconds	Suppression time in the range from 1 to 65535 in the unit of seconds.

Defaults The default is 60.

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# configure terminal
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** 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*]

Parameter Description

Parameter	Description
rp-address	IP address of RP
access_list	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 Examples The following example specifies the source IPv6 address of the register packet..

```
Ruijie# configure terminal
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 Description N/A

6.25 ip pim rp-candidate

Use this command to configure the C-RP. Use the **no** 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*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface number
priority-value	(Optional) Priority in the range 0 to 255, 192 by default
seconds	(Optional) Interval in the range 0 to 16383 seconds, 60s by default

access_list	(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 Mode Global configuration 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 Examples The following example configures the C-RP.

```
Ruijie# configure terminal
Ruijie(config)# ip pim rp-candidate g 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 Description N/A

6.26 ip pim rp-register-kat

Use this command to set the KAT interval on the RP. Use the **no** form of this command to restore the default setting.
ip pim rp-register-kat *seconds*
no ip pim rp-register-kat

Parameter Description

Parameter	Description
seconds	KAT timer time in the range from 1 to 65525 in the unit of seconds

Defaults The default is 210.

Command Mode Global configuration mode

Usage Guide This command is used to configure the KAT interval of RP.

Configuration Examples The following example sets the KAT interval on the RP to 250 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip pim rp-register-kat 250
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.27 ip pim sparse-mode

Use this command to enable PIM-SM on the interface. Use the **no** form of this command to restore the default setting.

ip pim sparse-mode

no ip 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-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 Examples The following example enables PIM-SM on the interface.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ip pim sparse-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.28 ip pim spt-threshold

Use this command to enable the SPT switching function. Use the **no** 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*]

Parameter Description

Parameter	Description
access_list	(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# configure terminal
Ruijie(config)# ip pim spt-threshold
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 Description N/A

6.29 ip pim ssm

Use this command to enable SSM and set the SSM group address range. Use the **no** form of this command to restore the default setting.

ip pim ssm { **default** | **range** *access_list* }

no ip pim ssm

Parameter Description

Parameter	Description
default	Multicast groups of 232/8
access_list	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# configure terminal
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

6.30 ip pim triggered-hello-delay

Use this command to configure Triggered-Hello-Delay time on the interface. Use the **no** form of this command to restore the default setting.

ip pim triggered-hello-delay *seconds*

no ip pim triggered-hello-delay

Parameter Description

Parameter	Description
interval-seconds	In the range from 1 to 5 in the unit of seconds.

Defaults The default is 5.

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 Examples The following command sets the triggered-hello-delay to 3 seconds.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ip pim triggered-hello-delay 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.31 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 Examples The following example displays the debugging status.

```
Ruijie # show debugging
PIM-SM Debugging status:
PIM packet debugging is on.
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

6.32 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
Next Cand_RP_advertisement in 00:00:32
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.33 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
interface-type interface-number	(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 Examples The following example displays the PIM-SM information on the interface.

```
Ruijie #show ip pim sparse-mode interface detail
GigabitEthernet 0/3 (vif 2):
  Address 30.30.100.200, DR 30.30.100.200
  Hello period 30 seconds, Next Hello in 13 seconds
  Triggered Hello period 5 seconds
  Neighbors:
   30.30.100.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.34 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
interface-type interface-number	(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 Examples The following example displays the local IGMP information on the PIM-SM interface.

```
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 Description N/A

6.35 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
group-or-source-address	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 Examples The following example displays the PIM-SM routing information.

```
Ruijie#show ip pim sparse-mode mroute
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.36 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 detail
Nbr 5.5.5.3 (VLAN 1)
  Expire in 81 seconds
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.37 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 This command displays the information on the next hop, including interface ID, IP address and metric.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.38 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
group-address	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 Examples The following example displays the RP information corresponding to the group address..

```
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 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 { *address* | **mapping** }

Parameter Description

Parameter	Description
address	Specifies the RP corresponding to the group.
mapping	All group and RP information.

Defaults N/A

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

Usage Guide This command displays the information on all RPs and the multicast groups they serve.

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 Description N/A

6.40 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
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 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_group_address ipv6_source_address* }

Parameter Description

Parameter	Description
*	Deletes all the multicast routing entries.
ipv6_group_address	Deletes the multicast routing entries of the specific group.
ipv6_group_address source_address	Deletes the multicast routing entries of the specific group and source IPv6 address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Multicast routing entries can be deleted manually.

Configuration Examples The following example clears the multicast routing entries.

```
Ruijie# clear ipv6 mroute *
Ruijie# clear ipv6 mroute ff66::6666
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 Description

Parameter	Description
*	Deletes the statistics of all multicast routing entries.

ipv6_group_address	Deletes the statistics of the multicast routing entries of the specific group.
ipv6_group_address ipv6_source_address	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 The statistics of multicast routing entries can be deleted manually.

Configuration Examples The following example deletes the statistics of the multicast routing entries.

```
Ruijie# clear ipv6 mroute statistics *
Ruijie# clear ipv6 mroute statistics ff66::6666
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 clears the RP information learnt dynamically.

clear ipv6 pim sparse-mode bsr rp-set *

Parameter Description

Parameter	Description
*	Clears all RP-SET.

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 the RP information learnt dynamically.

```
Ruijie# clear ipv6 pim sparse-mode bsr rp-set *
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

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 This command is used to reconfigure the start time of the statistics and clear the PIMv6 packet counter.

Configuration Examples The following example clears the PIMv6 packet counter.

```
Ruijie# clear ipv6 pim sparse-mode track
```

Related Commands	Command	Description
	show ipv6 pim sparse-mode track	N/A

Platform Description N/A

7.5 ipv6 pim accept-bsr list

Use this command to confine the BSR address range. Use the **no** form this command to restore the default setting.

ipv6 pim accept-bsrr list *ipv6_access-list*

no ipv6 pim accept-bsr

Parameter Description	Parameter	Description
	list *ipv6_access-list*	IPv6 standard name ACL

Defaults By default, the PIM-SMv6 router receives all external BSM packets

Command Mode Global configuration mode

Usage Guide Use this command to confine the range of the legal BSR.

Configuration Examples The following example confines the BSR address range.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim accept-bsr list bsr-list
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.6 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** form of this command to restore the default setting.

ipv6 pim accept-crp-with-null-group

no ipv6 pim accept-crp-with-null-group

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 Examples The following example receives the C-RP-ADV packets whose prefix-count is 0.

```
Ruijie (config)# configure terminal
Ruijie (config)# ipv6 pim accept-crp-with-null-group
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

7.7 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** form of this command to restore the default setting,
ipv6 pim accept-crp list *ipv6_access-list*
no ipv6 pim accept-crp

Parameter Description

Parameter	Description
list *ipv6_access-list*	Extended IPv6 ACL

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 Examples The following example confines the C-RP address range and the multicast group address range it serves..

```
Ruijie (config)# comfigure terminal
Ruijie (config)# ipv6 pim accept-crp list crp-list
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.8 ipv6 pim accept-register

Use this command to confine the address range of the (S,G) entry of the register packets. Use the **no** 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

Parameter Description

Parameter	Description
ipv6_access-list	Access control list supporting name ACL.
map-name	Defines the routing map rule

Defaults The range is not confined by default.

Command Mode Global configuration 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 Examples The following example confines the source IPv6 address of register packets on the RP.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim accept-register list register-access-list
Ruijie(config)# ipv6 access-list register-access-list
The following example denies the register message of the specified source
fe80::2d0:f8ff:fe22:33ad
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

7.9 ipv6 pim bsr-border

Use this command to configure the BSR border. Use the **no** form of this command to restore the default setting.

ipv6 pim bsr-border

no 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 Examples The following example sets the BSR border on the interface *g 0/3*.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ipv6 pim bsr-border
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.10 ipv6 pim bsr-candidate

Use this command to configure the C-BSR. Use the **no** 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

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and number.
hash-mask-length	(Optional) HASK mask length configured for electing the RP in the range from 0 to 128. The default is 126.
priority-value	(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-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 Examples The following example s configures the C-BSR.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim bsr-candidate g 0/3 30 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.11 ipv6 pim dr-priority

Use this command to configure the DR priority, Use the **no** form of this command to restore the default setting.
ipv6 pim dr-priority *priority-value*
no ipv6 pim dr-priority

Parameter Description

Parameter	Description
priority-value	The larger the value, the higher the priority is. The range is from 0 to 4294967294. 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 has 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 Examples The following example configures the DR priority.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ipv6 pim dr-priority 11234
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.12 ipv6 pim ignore-rp-set-priority

Use this command to ignore the RP priority. Use the **no** form of this command to restore the default setting.

ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority

Parameter Description

Parameter	Description
N/A	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 corresponding to the multicast group.

Configuration Examples The following example ignores the RP priority.

```
Ruijie# configure terminal
Ruijie(config-if)# ipv6 pim ignore-rp-set-priority
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.13 ipv6 pim jp-timer

Use this command to set the interval to send the join/prune message. Use the no form of this command to restore the default setting.

ipv6 pim jp-timer *seconds*

no ipv6 pim jp-timer

Parameter Description

Parameter	Description
seconds	Interval to send the join/prune message in the range from 1 to 65535 in the unit of seconds

Defaults The default is 60.

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** form of this command to restore the default setting.

ipv6 pim neighbor-filter *ipv6_access-list*

no ipv6 pim neighbor-filter *ipv6_access-list*

Parameter Description

Parameter	Description
ipv6_access_list	Access control list supporting name 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 block the neighbor address fe80::2d0:f8ff:fe22:33ad/128.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ipv6 pim neighbor-filter acl
Ruijie(config-if)# exit
Ruijie(config-if)# ipv6 access-list acl
The following example denies the neighbor fe80::2d0:f8ff:fe22:33ad
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** form of this command to restore the default setting.

ipv6 pim neighbor-tracking

no 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 Examples The following example disables join restraint on the interface.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ipv6 pim neighbor-tracking
```

Related Commands

Command	Description
ipv6 pim propagation-delay	N/A

Platform Description N/A

7.16 ipv6 pim override-interval

Use this command to set the override-interval on the interface, Use the **no** form of this command to restore the default setting.

ipv6 pim override-interval *milliseconds*

no ipv6 pim override-interval

Parameter Description

Parameter	Description
interval-milliseconds	In the range 1 to 65535 in the unit of milliseconds

Defaults The default is 2500.

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 to 3000 milliseconds.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config)# ipv6 pim override-interval 3000
```

Related Commands

Command	Description
ipv6 pim propagation-delay	N/A

Platform Description N/A

7.17 ipv6 pim probe-interval

Use this command to set the register probe interval. Use the **no** form of this command to restore the default setting.

ipv6 pim probe-interval *seconds*

no ipv6 pim probe-interval

Parameter Description

Parameter	Description
seconds	In the range from 1 to 65535 in the unit of seconds

Defaults The default is 5.

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 Examples The following example sets the probe time as 6 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim probe-interval 6
```

Related Commands

Command	Description
ipv6 pim register-suppression	N/A

Platform Description N/A

7.18 ipv6 pim propagation-delay

Use this command to set the propagation-delay on the interface. Use the **no** form of this command to restore the default setting.

ipv6 pim propagation-delay *milliseconds*
no ipv6 pim propagation-delay

Parameter Description

Parameter	Description
milliseconds	In the range from 1 to 32765 in the unit of milliseconds

Defaults The default is 500.

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# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config)# 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 pv6 pim query-interval

Use this command to set the interval to send the hellp packets. Use the **no** form of this command to restore the default setting.
ipv6 pim query-interval *seconds*
no ipv6 pim query-interval

Parameter Description

Parameter	Description
seconds	Interval to send the Hello message in the range from 1 to 65535 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# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config)# 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 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*]

Parameter Description

Parameter	Description
access-list	Access-list: access control list supporting name ACL. Group-list ipv6_access-list :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# configure terminal
```

```
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 Description N/A

7.21 ipv6 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.

ipv6 pim register-rate-limit *rate*

no ipv6 pim register-rate-limit

Parameter Description

Parameter	Description
rate	Maximum number of register packets that can be sent per second, in the range from 1 to 65535

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 Examples The following example limits the rate of register packets.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim register-rate-limit 3000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.22 ipv6 pim register-rp-reachability

Use this command to check RP reachability before sending register packets**.** Use the **no** form of this command to restore the default setting.

ipv6 pim register-rp-reachability

no 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# configure terminal
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** 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

Parameter Description

Parameter	Description
ipv6_local_address	Source IPv6 address of register packets
interface-type interface-number	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 Examples The following example configures the source IPv6 address of register messages.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim register-source 3333::3333
Ruijie(config)# ipv6 pim register-source g 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** form of this command to restore the default setting.
ipv6 pim register-suppression *seconds*
no ipv6 pim register-suppression

Parameter Description

Parameter	Description
seconds	Suppression time in the range from 1 to 65535 in the unit of seconds.

Defaults The default is 60.

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 Examples The following example sets the register packet suppression time.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim register-suppression 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.25 ipv6 pim rp-address

Use this command to configure the static RP. Use the **no** 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*]

Parameter Description

Parameter	Description
ipv6_rp-address	IPv6 address of RP
ipv6_access_list	Access control list supporting name ACL.

Defaults No IPv6 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 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 Examples The following example configures the RP static address.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim rp-address 3333::3333 acl
Ruijie(config)# ipv6 pim rp-address 210.34.0.55 4
Ruijie(config)# ipv6 access-list ac
Ruijie(config)# permit ipv6 any ff66::6666/64
```

Related Commands

Command	Description
ipv6 access-list	N/A

Platform Description N/A

7.26 ipv6 pim rp-candidate

Use this command to configure the C-RP. Use the **no** 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*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface number
priority-value	(Optional) Priority in the range from 0 to 255, 192 by default
interval-seconds	(Optional) Interval in the range from 0 to 16383 in the unit of seconds, 60 by default
ipv6_access_list	(Optional) ACL name. By default, all multicast groups are permitted.

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# configure terminal
Ruijie(config)# ipv6 pim rp-candidate g 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 Description N/A

7.27 ipv6 pim rp-register-kat

Use this command to set the survival time of (S, G) entry created by the register packet on the RP.
Use the **no** form of this command to restore the default setting.
ipv6 pim rp-register-kat *seconds*
no ipv6 pim rp-register-kat

Parameter Description

Parameter	Description
seconds	KAT timer time in the range from1 to 65525 in the unit of seconds.

Defaults The default is equal to the sum of register probe time and three times register suppression time.

Command Mode Global configuration mode

Usage Guide This command is used to configure the KAT interval of RP.

Configuration Examples The following example configures the KAT interval of RP.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim rp-register-kat 250
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

7.28 ipv6 pim rp embedded

Use this command to enable the embedded RP function. Use the **no** form of this command to disable this function.

ipv6 pim rp embedded [**group-list** *ipv6_acl_name*]

no ipv6 pim rp embedded

Parameter Description

Parameter	Description
group-list *ipv6_acl_name*	Enables embedded RP for the IPv6 multicast address of specified embedded RP address.

Defaults This function is disabled 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	N/A

Platform Description N/A

7.29 ipv6 pim sparse-mode

Use this command to enable PIM-SMv6 on the interface. Use the **no** form of this command to restore the default setting.

ipv6 pim sparse-mode

no 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.

Configuration Examples The following example enables PIM-SMv6 on the interface.

```
Ruijie# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ipv6 pim sparse-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.30 ipv6 pim spt-threshold

Use this command to enable SPT switch. Use the **no** 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*]

Parameter Description

Parameter	Description
ipv6_access_list	(Optional) supporting 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 switch.

```
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

7.31 ipv6 pim ssm

Use this command to enable SSM and set the SSM group address range. Use the **no** form of this command to restore the default setting.

ipv6 pim ssm { **default** | **range** *ipv6_access-list* }

no ipv6 pim ssm

Parameter Description

Parameter	Description
default	Group in the range of FF3x::/32
range *ipv6_access_list*	Supporting name ACL.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable PIM-SSMv6 (or in some specific multicast groups).

Configuration Examples The following example sets the source-specific multicast of the multicast group range acl.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim ssm range acl
```

The following example uses SSM for the source address fe80::2d0:f8ff:fe22:33ad, group range of ff32::3333/64.

```
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 Description N/A

7.32 ipv6 pim static-rp-preferred

Use this command to configure a higher priority for static RP over the C-RP, Use the **no** form of this command to restore the default setting.

ipv6 pim static-rp-preferred

no 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 Mode Interface configuration mode

Usage Guide With this command configured, the priority of the static RP is higher than the one elected through the BSR mechanism.

Configuration Examples The following example configures the priority of the static RP is higher than the one elected through the BSR mechanism.

```
Ruijie# configure terminal
Ruijie(config-if)# ipv6 pim static-rp-preferred
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

7.33 ipv6 pim triggered-hello-delay

Use this command to configure Triggered-Hello-Delay time on the interface. Use the **no** form of this command to restore the default setting.

ipv6 pim triggered-hello-delay *seconds*

no ipv6 pim triggered-hello-delay

Parameter Description

Parameter	Description
seconds	In the range from1 to 5 in the unit of seconds.

Defaults The default is 5.

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# configure terminal
Ruijie(config)# interface g 0/3
Ruijie(config-if)# ipv6 pim triggered-hello-delay 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.34 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 Examples The following example displays the debugging status.

```
Ruijie # show debugging
PIM-SM Debugging status:
PIM packet debugging is on.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.35 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 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 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 Description N/A

7.36 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
interface-type interface-number	(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-SMv6 information on the interface.

Configuration Examples The following example displays the PIM-SMv6 interface information.

```
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 Description N/A

7.37 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
interface-type interface-number	(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 MLD information on the PIM-SMv6-enabled interface.

Configuration Examples The following example displays the local MLD information on the PIM-SMv6 interface.

```
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 Description N/A

7.38 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 Description

Parameter	Description
group-or-source-address	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 Description N/A

7.39 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 Description N/A

7.40 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 This command displays the information on the next hop, including interface number, IP address and metric.

Configuration Examples N/A

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.41 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	Parameter	Description

Description

mapping	All groups and RP information.

Defaults N/A

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

Usage Guide This command displays the information on all RPs and the multicast groups they serve.

Configuration Examples The following example displays the information on all RPs and the multicast groups they serve.

```
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 Description N/A

7.42 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
ipv6_group-address	IPv6 group address

Defaults N/A

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

Usage Guide This command displays the information on the RP of the specific group IPv6 address.

Configuration Examples The following example displays the RP information corresponding to the group address..

```
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 Description N/A

7.43 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 GDA table.

clear ip igmp snooping gda-table

Parameter Description

Parameter	Description
N/A	N/A

Default N/A

Command Mode Privileged EXEC mode

Usage Guide The GDA table entry includes VLAN ID, group destination address, routing interface, and member port.
The VLAN ID and the group destination address identify a forwarding entry.
One forwarding entry may contain multiple routing interfaces (dynamic routing interfaces or static routing interfaces). The static routing interface is not aged.
One forwarding entry may contain multiple member ports (dynamic member ports or static member ports). The static member is not aged. Executing the **clear ip igmp snooping gda-table** command will not delete the static member ports.

Configuration Example The following example clears the GDA table.
Ruijie# clear ip igmp snooping gda-table

Related command

Command	Description
N/A	N/A

Platform Description N/A

8.2 clear ip igmp snooping statistics

Use this command to clear the IGMP snooping statistics.

clear ip igmp snooping statistics

Parameter Description

Parameter	Description
N/A	N/A

Default N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the IGMP snooping statistics.

Configuration Examples The following example clears the IGMP snooping statistics.

```
Ruijie# clear ip igmp snooping statistics
```

Related command

Command	Description
N/A	N/A

Platform Description N/A

8.3 deny

Use this command to deny the forwarding of the multicast streams in the range specified by the profile.

deny

Parameter Description N/A

Defaults This function is disabled by default.

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 example denies the forwarding of the multicast stream 224.2.2.2.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2
Ruijie(config-profile)# deny
```

Related Commands

Command	Description
ip igmp profile	Creates a profile.
range	Configures the multicast address range.

8.4 ip igmp profile

Use this command to select a profile and enter the IGMP profile configuration mode. Use the no form of this command to restore the default setting.

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

Parameter Description

Parameter	Description
profile-number	Profile number, in the range from 1 to 65535

Defaults N/A

Command Mode Global configuration mode

Usage Guide The profile must be applied to the specified interface in order to make the profile take effect.

Configuration Examples

The following example shows how to create a profile numbered 1 and enter the profile configuration mode.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)#
```

Related Commands

Command	Description
range	Configures the multicast address range.

8.5 ip igmp snooping

Use this command to enable IGMP Snooping and set IVGL/SVGL/IVGL-SVGL mode. Use the **no** or **default** form of this command to restore the default setting.

ip igmp snooping ivgl

ip igmp snooping svgl

ip igmp snooping ivgl-svgl

no ip igmp snooping

default ip igmp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration 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.

The SVGL mode and IVGL-SVGL mode are not compatible with the IP multicast function.

The PIM Snooping function is based on IGMP Snooping IVGL mode or IVGL-SVGL mode. If you want to disable IGMP Snooping when PIM Snooping is running, the operation fails and you should disable PIM Snooping first.

Configuration Examples

The following example enables IGMP Snooping IVGL mode.

```
Ruijie(config)# ip igmp snooping ivgl
```

The following example enables IGMP Snooping SVGL mode and specifies the shared VLAN and SVGL group range as VLAN1 and profile1 respectively.

```
Ruijie(config)# ip igmp snooping svgl
Ruijie(config)# ip igmp snooping svgl profile 1
```

The following example enables IGMP Snooping IVGL-SVGL mode and specifies the shared VLAN and SVGL group range as VLAN1 and profile1 respectively.

```
Ruijie(config)# ip igmp snooping ivgl-svgl
Ruijie(config)# ip igmp snooping svgl profile 1
```

Related Commands

Command	Description
N/A	N/A

8.6 ip igmp snooping dyn-mr-aging-time

Use this command to configure the aging time of the routing interface that the switch learns dynamically. Use the no form of this command to restore the default setting.

ip igmp snooping dyn-mr-aging-time *time*

no ip igmp snooping dyn-mr-aging-time

Parameter Description

Parameter	Description
time	Aging time of the routing interface that the switch learns dynamically, in the range from 1 to 3600 in the unit of seconds.

Defaults The default is 300.

Command Mode Global configuration mode

Usage Guide 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
```

Related Commands	Command	Function
	ip igmp snooping	Enables IGMP snooping.

8.7 ip igmp snooping fast-leave enable

Use this command to enable the fast leave function. Use the **no** form of this command to restore the default setting.

ip igmp snooping fast-leave enable

no 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 Examples The following example enables the fast leave function on the switch.

```
Ruijie(config)# ip igmp snooping fast-leave
```

Related Commands	Command	Function
	N/A	N/A

8.8 ip igmp snooping filter

Use this command to configure a port to receive a specific set of multicast streams. Use the **no** form of this command to restore the default setting.

ip igmp snooping filter *profile-number*

no ip igmp snooping filter *profile-number*

Parameter Description	Parameter	Description
	profile-number	Profile number

Defaults N/A

Command Mode Global configuration mode / Interface configuration mode.

Usage Guide A specific profile must be created before association.

Configuration Examples The following example associates profile 1 to a megabit port 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

Related Commands

Command	Description
ip igmp profile	Creates a profile.

8.9 ip igmp snooping host-aging-time

Use this command to configure the aging time of IGMP dynamic ports. Use the **no** form of this command to restore the default setting.

ip igmp snooping host-aging-time *seconds*

no ip igmp snooping host-aging-time

Parameter Description

Parameter	Description
seconds	Aging time, in the range from 1 to 65535 in the unit of seconds.

Defaults The default is 260.

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 Examples The following example sets the aging time to 30 seconds.

```
Ruijie(config)# ip igmp snooping host-aging-time 30
```

Related command

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** form of this command to restore the default setting.

ip igmp snooping l2-entry-limit *number*

no ip igmp snooping l2-entry-limit

Parameter Description

Parameter	Description
number	Number of multicast groups, in the range from 0 to 4096.

Defaults The default is 1024.

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.

```
Ruijie(config)# ip igmp snooping l2-entry-limit 2000
```

Related command

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** form of this command to restore the default setting.

ip igmp snooping limit-ipmc vlan *vid* **address** *group-address* **server** *source-address*

no ip igmp snooping limit-ipmc vlan *vid* **address** *group-address*

Parameter Description

Parameter	Description
vid	VLAN ID of the source IP address check entry
group-address	Multicast address
source-address	Multicast source IP address (multicast server)

Defaults N/A

Command Mode Global configuration mode

Usage Guide The source IP address check function must be enabled before an entry can be added.

Configuration Examples The following example adds an entry to the multicast source IP address check table.

```
Ruijie(config)# ip igmp snooping limit-ipmc vlan 1 address 224.0.0.1
server 192.168.4.243
```

Related Commands

Command	Description
ip igmp snooping source-check default-server	Configures a default source IP address while enabling the IP check function.

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** form of this command to restore the default setting.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

Parameter Description

Parameter	Description
number	The parameter is in the range from 0 to 1024.

Defaults The default is 1024.

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 Examples The following example configures the maximum number of multicast groups to 100 on the megabit interface 0/1.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping max-group 100
```

Related Commands

Command	Description
ip igmp snooping filter	Filters multicast groups that pass through a port.

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 this function.

ip igmp snooping mrouter learn pim-dvmrp

no ip igmp snooping mrouter learn pim-dvmrp

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 neighboring 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 Examples The following example enables the dynamic routing interface learning function on the equipment.

```
Ruijie(config)# ip igmp snooping mrouter learn pim-dvmrp
```

Related Commands

Command	Description
ip igmp snooping vlan mrouter learn pim-dvmrp	Enables the dynamic routing interface learning function on the multicast routing port.

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** form of this command to restore the default setting,

ip igmp snooping preview *profile-number*

no ip igmp snooping preview

Parameter Description

Parameter	Description
profile-number	Profile number is in the range from 1 to 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 1 to the 100M port 0/1 and associates multicast preview with profile 2.

```
Ruijie(config)# ip igmp snooping preview 2
Ruijie(config-if)# int fa 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

Related Commands

Command	Description
ip igmp profile	Creates a profile

Platform Description N/A

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 the **no** form of this command to restore the setting.

ip igmp snooping preview interval *seconds*

no ip igmp snooping preview interval

Parameter Description

Parameter	Description
seconds	Preview interval, in the range from 1 to 300 in the unit of seconds.

Defaults The default is 60.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the multicast preview interval to 100 seconds on the 100M port of 0/1.

```
Ruijie(config)# ip igmp snooping preview interval 100
```

Related Commands

Command	Description
ip igmp snooping preview	Enables the multicast preview.

Platform Description N/A

8.16 ip igmp snooping querier

Use this command to enable the IGMP querier function, execute "**ip igmp snooping querier**" global configuration command. Use **no** form of this command to restore the default setting.

ip igmp snooping querier

no ip igmp snooping querier

Parameter Description	**Parameter**	**Description**
	N/A	N/A

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 affect this command.
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 on the device.

```
Ruijie(config)# ip igmp snooping querier
```

Related Commands	**Command**	**Description**
	ip igmp snooping vlan querier	Enables the querier function in VLAN

Platform Description N/A

8.17 ip igmp snooping querier address

Use this command to enable the IGMP querier, you also need to specify a source IP address for query packets. Use the **no** form of this command to restore the default setting.

ip igmp snooping querier address *a.b.c.d*

no ip igmp snooping querier address

Parameter Description	**Parameter**	**Description**
	a.b.c.d	Source IP address of the query packets.

Defaults No source IP address is specified

Command Mode	Global configuration mode
Usage Guide	After enabling IGMP querier, you also need to configure a source IP address for query packets, so that the device can send packets normally. If no source IP address is specified in the VLAN needing to send packets, the device will verify whether the source IP address is specified globally. The device can only send query packets after finding the source IP configured, or else the querier function won't take effect. If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.
Configuration Examples	The following example specifies the source IP of query packets on the device. `Ruijie(config)# ip igmp snooping querier address 1.1.1.1`

Related Commands

Command	Description
ip igmp snooping vlan querier address	Enables the source IP check in VLAN

Platform Description	N/A

8.18 ip igmp snooping querier max-response-time

Use this command to configure the maximum response time advertised in query packets. Use **no** form of this command to restore the default setting.

ip igmp snooping [**vlan** *vid*] **querier max-response-time** *seconds*

no ip igmp snooping [**vlan** *vid*] **querier max-response-time**

Parameter Description

Parameter	Description
VLAN *vid*	Specifies a VLAN.
seconds	Maximum response time, in the range from 1 to 25 in the unit of seconds.

Defaults	The default time is 10 seconds.
Command Mode	Global configuration mode
Usage Guide	Configure this command to specify the maximum response time to query packets. 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.
Configuration	The following example specifies the maximum response time to query packets on the device.

Examples

```
Ruijie(config)# ip igmp snooping querier max-response-time 15
```

Related Commands

Command	Description
ip igmp snooping vlan querier max-response-time	Configures the maximum response time to query packets in VLAN

Platform Description N/A

8.19 ip igmp snooping querier query-interval

Use this command to specify the interval for IGMP querier to send query packets. Use **no** form of this command to restore the default setting.

ip igmp snooping [**vlan** *vid*] **querier query-interval** *seconds*

no ip igmp snooping [**vlan** *vid*] **querier query-interval**

Parameter Description

Parameter	Description
VLAN *vid*	Specifies a VLAN.
seconds	Maximum response time, in the range from 1 to 18000 in the unit of seconds.

Defaults The default is 60.

Command Mode Global configuration mode

Usage Guide

After globally enabling IGMP querier, the timer will be enabled for sending query packets periodically. The aging time of the timer is the query interval. Configure this command to change the query interval.

If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Configuration Examples The following example configures the query interval on the device.

```
Ruijie(config)# ip igmp snooping querier query-interval 100
```

Related Commands

Command	Description
ip igmp snooping vlan querier query-interval	Configures the query interval in VLAN

Platform Description N/A

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 to the default setting.

ip igmp snooping [**vlan** *vid*] **querier timer expiry** *seconds*

no ip igmp snooping [**vlan** *vid*] **querier timer expiry**

Parameter Description

Parameter	Description
vlan *vid*	Specifies a VLAN.
seconds	Maximum response time, in the range from 60 to 300 in the unit of seconds.

Defaults The default is 125.

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
```

Related Commands

Command	Description
ip igmp snooping vlan querier timer expiry	Configures querier expiration timer in VLAN

Platform Description N/A

8.21 ip igmp snooping querier version

Use this command to specify the version. Use **no** form of this command to restore the default setting.

ip igmp snooping querier version *num*

no ip igmp snooping querier

Parameter Description

Parameter	Description
num	IGMP version number (1-2).

Defaults The default is IGMPv2.

Command Mode	Global configuration mode
Usage Guide	If the IGMP querier version number has been configured in the corresponding VLAN, the value specified in VLAN will be used first.
Configuration Examples	The following example configures IGMP querier version on the device. `Ruijie(config)# ip igmp snooping querier version 1`

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.22 ip igmp snooping query-max-response-time

Use this command to configure the maximum response time of the query packets. Use the no form of this command to restore the default setting..

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time

Parameter Description

Parameter	Description
seconds	The aging time of the routing interface that the switch learns dynamically, in the range from 1 to 65535 in the unit of seconds.

Defaults The default is 10.

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 example 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
```

Related Commands

Command	Function
ip igmp snooping	Configures a multicast routing interface.

8.23 ip igmp snooping source-check default-server

The source IP address check is used to permit one or several IPMC flows from the server of the specified IP address.
To configure the source IP address check function of IGMP snooping, execute the **ip igmp snooping source-check default-server** command in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip igmp snooping source-check default-server *address*

no ip igmp snooping sauce-check

Parameter Description

Parameter	Description
address	Default multicast source IP address (IP address of the default multicast server)

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. 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 Examples The following example enables the multicast source IP address check function and configures a default source IP address.

```
Ruijie(config)# ip igmp snooping source-check default-server
192.168.4.243
```

Related Commands

Command	Description
Ip igmp snooping limit-ipmc vlan server	Adds an entry to the source IP check table.

8.24 ip igmp snooping source-check port

The source port check function is used to permit one or several IPMC flows from the mroute port.
Use this command to configure the source port check function of IGMP snooping, execute the **ip igmp snooping source-check port** command in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip igmp snooping source-check port

no ip igmp snooping source-check port

Parameter Description N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The source port check function takes effect globally. Once it is enabled, only the IPMC streams from the specified port are permitted.

Configuration Examples The following example enables the source port check function of IGMP snooping.

```
Ruijie(config)# ip igmp snooping source-check port
```

Related Commands

Command	Description
Ip igmp snooping source-check default-server	Enables the multicast source IP address check function.

8.25 ip igmp snooping suppression enable

To enable IGMP snooping suppression, execute the **ip igmp snooping suppression enable** command in the global configuration mode. Use the **no** form of this command to restore the default setting.

ip igmp snooping suppression enable

no ip igmp snooping suppression enable

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 suppression function, the switch begins to suppress the IGMP v1/v2 report messages.

Configuration Examples The following example enables IGMP snooping suppression on the device.

```
Ruijie(config)# ip igmp snooping suppression
```

Related Commands N/A

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** form of this command to restore the default setting.

ip igmp snooping profile *profile-number*

no ip igmp snooping profile

Parameter Description

Parameter	Description

profile-number	Profile number, in the range from 1 to 1024.

Defaults No profile is associated by default.

Command Mode Global configuration mode

Usage Guide When the IGMP Snooping works in the SVGL or 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. By default, no profile is associated.

Configuration Examples The following example specifies the multicast group address range.

```
Ruijie(config)# ip igmp snooping svgl profile 1
```

Related Commands

Command	Description
ip igmp snooping ivgl	Enables igmp snooping and enters the IVGL mode.
ip igmp snooping ivgl-svgl	Enables igmp snooping and enters the hybrid mode

8.27 ip igmp snooping svgl subvlan

Use this command to specify the subvlan of multicast VLAN. Use the **no** form of this command to restore the default setting.

ip igmp snooping svgl subvlan [*vid-range*]

no ip igmp snooping svgl subvlan [*vid-range*]

Parameter Description

Parameter	Description
vid-range	VLAN ID or range of VLAN ID

Defaults By default, no subvlan is specified for svgl, and all VLANs serve as its subvlans.

Command Mode Global configuration mode

Usage Guide This command only takes effect in SVGL or IVGL-SVGL mode.

Configuration Examples The following example configures the device operating in igmp snooping svgl mode to associate VLAN 2, 5, 6 and 7.

```
Ruijie(config)# ip igmp snooping svgl vlan 2,5-7
```

Related Commands

Command	Description
ip igmp snooping svgl	Enables the igmp snooping and configures the svgl mode.

ip igmp snooping ivgl-svgl	Enables the igmp snooping and configures the IVGL-SVGL mode.
ip igmp snooping svgl vlan	Configures the primary VLAN of SVGL mode.

Platform Description N/A

8.28 ip igmp snooping svgl vlan

Use this command to specify the vlan as the shared vlan in the 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

Parameter Description

Parameter	Description
vid	VLAN ID.

Defaults By default , the shared vlan is vlan1.

Command Mode Global configuration mode

Usage Guide This command only works in the SVGL or IVGL-SVGL mode.

Configuration Examples The following example specifies the vlan2 as the shared vlan

```
Ruijie(config)# ip igmp snooping svgl vlan 2
```

Related Commands

Command	Description
ip igmp snooping svgl	Enables igmp snooping and enters the SVGL mode.
ip igmp snooping ivgl-svgl	Enables igmp snooping and enters the hybrid mode

8.29 ip igmp snooping tunnel

Configure the relationship between IGMP Snooping and QinQ. Use the **no** form of this command to restore the default setting,

ip igmp snooping tunnel

no ip igmp snooping tunnel

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

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 through IGMP Snooping: 1st way: Create multicast entries in the VLAN to which the IMGP packets belong, and forward IMGP packets in such 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 can pass through 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. 2nd way: 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 can pass through 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 2nd way is used.
Configuration Examples	The following example enables the IGMP packets transparent transmission on the device. `Ruijie(config)# ip igmp snooping tunnel`

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

8.30 ip igmp snooping vlan

Use this command to enable the igmp snooping on the specified vlan and enter the ivgl mode. Use the **no** form of this command to restore the default setting.

ip igmp snooping vlan *vid*

no ip igmp snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID

Defaults	This function 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 on the specified vlan works only when the igmp snooping configured. when disabling the igmp snooping on the vlan with the pim snooping configured, it prompts to disable the pim snooping first and this execution fails.

Configuration Examples The following example enables the igmp snooping on the vlan2.

```
Ruijie(config)# ip igmp snooping vlan 2
```

Related Commands

Command	Description
ip igmp snooping ivgl	Enables the igmp and enters the ivgl mode
ip igmp snooping ivgl-svgl	Enables the igmp snooping and enters the ivgl-svgl mode

8.31 ip igmp snooping vlan mrouter interface

Routing interface is a port through which a multicast device is directly connected to a multicast neighboring device. Use this command to configure a multicast routing interface. Use the **no** form of this command to restore the default setting.

ip igmp snooping vlan *vid* **mrouter interface** *interface-id*

no ip igmp snooping vlan *vid* **mrouter interface** *interface-id*

Parameter Description

Parameter	Description
vid	VLAN ID of a routing interface
interface-id	Interface ID

Defaults No static route interface is configured by default.

Command Mode Global configuration mode

Usage Guide 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 Examples The following example configures a multicast routing interface on the equipment.

```
Ruijie(config)# ip igmp snooping vlan 1 mrout erinterface
fastEthernet 0/1
```

Related Commands

Command	Description
ip igmp snooping source-check port	Enables the multicast source port check function.

8.32 ip igmp snooping vlan static interface

Use this command to configure a static interface within the group. Use the **no** form of this command to restore the default setting.

ip igmp snooping vlan *vid* **static** *ip-addr* **interface** *interface-id*

no ip igmp snooping vlan *vid* **static** *ip-addr* **interface** *interface-id*

Parameter Description

Parameter	Description
vid	VLAN ID of a routing interface
ip-addr	Multicast IP address
interface-id	Interface ID

Defaults N/A

Command Mode Global configuration mode

Usage Guide Multiple multicast IP addresses can be configured for an interface.

Configuration Examples The following example configures a static multicast address on a port.

```
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface
GigabitEthernet 0/1
```

Related Commands

Command	Description
ip igmp snooping vlan mdevice interface	Configures a multicast routing interface

8.33 permit

Use this command to permit the forwarding of the multicast streams in the range specified by the profile. In this way, the interface associated with this profile will forward the specified multicast stream only.

permit

Parameter Description 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 to take effective.

Configuration Examples The following example allows the forwarding of the multicast stream 224.2.2.2.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2
```

```
Ruijie(config-profile)# permit
```

Related Commands	Command	Description
	ip igmp profile	Creates a profile.
	range	Configures the multicast address range.

8.34 range

Use this command to specify the range of multicast streams. You can specify either a single multicast address or a range of multicast addresses. Use the **no** form of this command to restore the default setting.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter Description	Parameter	Description
	low-ip-address	Start address of a range
	high-ip-address	End address of a range

Defaults N/A

Command Mode Profile configuration mode

Usage Guide You can specify a behavior after configuring the address range, for example deny by default. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Configuration Examples The following example creates a profile whose multicast stream is in the range 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
```

Related Commands	Command	Description
	ip igmp profile	Creates a profile.
	deny	Denies the forwarding of the multicast streams in the range specified by the profile.
	permit	Permits the forwarding of the multicast streams in the range specified by the profile.

8.35 show ip igmp profile

Use this command to display the profile information.

show ip igmp profile [*profile-number*]

Parameter Description

Parameter	Description
profile-number	Displays configuration information of the designated profile, in the range from 1 to 1024.

Command Mode Privileged EXEC mode

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** | **mdevice**| **statistics** [**vlan** *vlan-id*]]

Parameter Description

Parameter	Description
none	Displays the function configuration of IGMP snooping.
gda-table	Displays multicast forwarding rule table.
interfaces	Displays the configuration of igmp snooping filtring
mdevice	Displays interface configuration of multicast device.
statistics [**vlan** *vlan-id*]	Displays the igmp snooping statistics.

Command Mode Privileged EXEC mode

Configuration Examples

The following example processes 100 multicast groups on the interface fa0/1.

```
Ruijie(config-if)# ip igmp snooping gda-table
Abbr:M - mrouter
D - dynamic
S - static
VLAN Address Member ports
----------------------------------------
1 233.3.3.3 Gi0/2(S)
2 234.4.4.4 Gi0/11(S)
1 233.4.4.4 Ag2(S)
```

Security Configuration Commands

1 AAA Commands

1.1 aaa accounting commands

	Use this command to account users in order to count the network access fees or manage user activities. 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 Description	**Parameter**	**Description**
	level	The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.
	default	When this parameter is used, the following defined method list is used as the default method for command accounting.
	list-name	Name of the command accounting method list, which could be any character strings.
	method	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 Examples	The following example performs accounting of the network service requests from users using TACACS+, and sets the accounting command level to 15. `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 Description	N/A	

1.2 aaa accounting exec

	Use this command to account users in order to count the network access fees or manage user activities. 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 Description	**Parameter**	**Description**
	default	When this parameter is used, the following defined method list is used as the default method for Exec accounting.
	list-name	Name of the Exec accounting method list, which could be any character strings.
	method	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 Mode	Global configuration 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 Examples	The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access. `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 Description	N/A	

1.3 aaa accounting network

	Use this command to account users in order to count the network access fees or manage user activities. Use the **no** form of this command to restore the default setting.	
	aaa accounting exec network { **default |** *list-name* } **start-stop** *method1* [*method2*..]	
	no aaa accounting exec network { **default**	*list-name* }	
Parameter Description	**Parameter**	**Description**
	default	When this parameter is used, the following defined method list is used as the default method for Network accounting.
	list-name	Name of the accounting method list
	start-stop	Count the network access fees from the beginning to end.
	method	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 performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access. `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 Description	N/A	

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 Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration 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 Examples	The following example enables the accounting update function. `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 Description	N/A	

1.5 aaa accounting update periodic

	If the accounting update function has been enabled, use this command to set the interval of sednign 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 Description	**Parameter**	**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.	
Command Mode	Global configuration 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 Examples	The following example sets the interval of accounting update to 1 minute. `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 Description	N/A	

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.
	list-name	Name of the 802.1x user authentication method list, which could be any character string.
	method	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 Mode	Global configuration 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 Description	N/A	

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** | *list-name* } *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.
	method	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.

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 Description	N/A

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.
	list-name	Name of the user authentication method list, which could be any character strings.
	method	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.
Defaults	N/A	
Command Mode	Global configuration 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 Description	N/A	

1.9 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.
	list-name	Name of second-generation Web authentication method list, which could be any character strings.

	method	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.
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	

1.10 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**
	level	Command level to be authorized, 0-15.
	default	When this parameter is used, the following defined method list is used as the default method for command authorization.
	list-name	Name of the user authorization method list, which could be any character strings.
	method	It must be one of the keywords: **none** and **group**. One method list can contain

		up to four methods.
	none	Dose 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 Examples	The following example uses the TACACS+ server to authorize the level 15 command: `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 Description	N/A	

1.11 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 resotre 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 Examples	The following example enables the configuration command authorization function. `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 Description	N/A

1.12 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 Description	**Parameter** / **Description** N/A / N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration 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 Examples	The following example enables the aaa authorization console function. `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 Description	N/A	

1.13 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 Description	**Parameter**	**Description**
	default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
	list-name	Name of the user authorization method list, which could be any character strings.
	method	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 Mode	Global configuration 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 can not 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 Examples	The following example uses the RADIUS server to authorize Exec. `Ruijie(config)# aaa authorization exec default group radius`	
Related Commands	**Command**	**Description**
	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 Description	N/A

1.14 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 Description	**Parameter**	**Description**
	default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
	method	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	

1.15 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 Description	**Parameter**	**Description**
	default	Uses this parameter to configure the default domain.
	domain-name	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 Examples	The following example configures the domain name. `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 Description	N/A	

1.16 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 Description	**Parameter**	**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 Examples	The following example enables the domain-name-based AAA service. `Ruijie(config)# aaa domain enable`

Related Commands	**Command**	**Description**
	aaa new-model	Enables the AAA security service.
	show aaa doamain	Displays the domain configuration.

Platform Description	N/A

1.17 aaa local authentication attempts

	Use this command to set login attempt times.
	aaa local authentication attempts *max-attempts*

Parameter Description	**Parameter**	**Description**
	max-attempts	In the range from 1 to 2147483647.

Defaults	The default is 3.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure login attempt times.
Configuration Examples	The following example sets login attempt times to 6. `Ruijie #configure terminal`

	`Ruijie (config)#aaa local authentication attempts 6`
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

1.18 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 Description	**Parameter** / **Description**
	lockout-time / In the range from 1 to 2147483647 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

1.19 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 disable the system to print the system informing AAA

	authentication success.
	aaa log enable
	no aaa log enable

Parameter Description	**Parameter**	**Description**
	N/A	N/A

Defaults	This function is enabled 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 Examples	The following example disables the system to print the syslog informing aaa authentication success.. `Ruijie(config)# no aaa log enable`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

1.20 aaa log rate-limit

	Use this command to set the rate of printing the syslog informing AAA authentication success. Use the **no** form of this command to restore the default printing rate.
	aaa log rate-limit *num*
	no aaa log rate-limit

Parameter Description	**Parameter**	**Description**
	num	The number of syslog entries printed per second. The range is from 0 to 655,535. 0 indicates the printing rate is not limited. The default is 5.

Defaults	The default is 5.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Examples	The following example sets the rate of printing the syslog informing AAA authentication success to 10. `Ruijie(config)# aaa log rate-limit 10`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

1.21 aaa new-model

	Use this command to enable the RGOS AAA security service. Use the **no** form of this commandto 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 Examples	The following example enables the AAA security service. `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 Description	N/A

1.22 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 Description	**Parameter**	**Description**
	num	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 Mode	Domain configuration mode	
Usage Guide	This command limits the number of users for the domain.	
Configuration Examples	The following example sets the number of users to 20 for the domain named ruijie.com. `Ruijie(config)# aaa domain ruijie.com` `Ruijie(config-aaa-domain)# access-limit 2`	
Related Commands	**Command**	**Description**
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Switchover the user level.
	show aaa domain	Defines a local user database.
Platform Description	N/A	

1.23 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 Description	**Parameter**	**Description**
	default	Uses this parameter to specify the default method list.
	list-name	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 Mode	Domain configuration mode
Usage Guide	Use this command to configure the Network accounting method list for the specified domain.
Configuration Examples	The following example sets the Network accounting method list for the specified domain. `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 Description	N/A

1.24 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 Description	**Parameter**	**Description**
	default	Uses this parameter to specify the default method list
	list-name	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 IEEE802.1x authentication method list for the domain.
Configuration Examples	The following example sets an IEEE802.1x authentication method list for the specified domain. `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 Description	N/A

1.25 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 Description	**Parameter** / **Description**
	default / Uses this parameter to specify the default method list.
	list-name / 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 Examples	The following example sets an authorization method list for the specified domain. `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 Description	N/A

1.26 clear aaa local user lockout

	Use this command to clear the lockout user list.	
	clear aaa local user lockout { **all	user-name** *word* }	
Parameter Description	**Parameter**	**Description**
	all	Indicates all locked users.
	user-name *word*	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 the specified user list.	
Configuration Examples	The following example clears the lockout user list. `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	

1.27 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 Examples	The following example displays the accounting update information. `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	

1.28 show aaa domain

	Use this command to display all current domain information.	
	show aaa domain [**default** | *domain-name*]	
Parameter Description	**Parameter**	**Description**
	default	Displays the default domain.
	domain-name	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 Examples	The following example displays the domain named domain.com. `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 Description	N/A	

1.29 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 Examples	The following example displays the lockout configuration. `Ruijie# show aaa lockout` `Lock tries:  3` `Lock timeout:  15 minutes`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

1.30 show aaa group

	Use this command to display all the server groups configured for AAA.	
	show aaa group	
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 command displays all the server groups. `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 Description	N/A

1.31 show aaa method-list

	Use this command to display all AAA method lists.
	show aaa method-list

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 all AAA method lists.
Configuration Examples	The following example displays the AAA method list. `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 authorizating network default group radius

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 Description	N/A

1.32 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 Description	**Parameter**	**Description**
	all	Displays all AAA user information.
	lockout	Displays the locked AAA user information.
	by-id *session-id*	Displays the information of the AAA user that with a specified session ID.
	by-name *user-name*	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 Description	N/A	

1.33 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 Description	**Parameter**	**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 Description	N/A

1.34 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 Description	**Parameter**	**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 Mode	Domain configuration 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 Examples	The following example sets the user name without the domain information. `Ruijie(config)# aaa domain ruijie.com` `Ruijie(config-aaa-domain)# username-domain without-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 Description	N/A	

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**
	name	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 radius source-interface

	Use this command to specify the source IP address for the RADIUS packets. 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 Description	**Parameter**	**Description**
	interface-name	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 Mode	Global configuration 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 Description	N/A	

2.3 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	**Parameter**	**Description**

Description		
	vrf_name	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 Description	N/A	

2.4 radius attribute

	The following example sets the private attribute type value. Use the **no** form of this command to restore the default setting.	
	radius attribute { *id* **| down-rate-limit | dscp | mac-limit | up-rate-limit** } **vendor-type** *type*	
	no radius attribute { *id* | **down-rate-limit** | **dscp** | **mac-limit | up-rate-limit** } **vendor-type**	
Parameter Description	**Parameter**	**Description**
	id	Function ID, in the range from 1 to 255
	type	Private attribute type, in the range from 1 to 255.
Defaults	Only the default configuration of private attributes in Ruijie is recognized.	

id	Function	type
1	max down-rate	1
2	q s	2

3	user ip	3
4	vlan id	4
5	Version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
2	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	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42

Extended attributes:

id	Function	type
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
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	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Command Mode	Global configuration mode
Usage Guide	This command is used to configure the private attribute type value.
Configuration Examples	The following example sets the type of max up-rate to 211. `Ruijie(config)# radius attribute 16 vendor-type 211`

Related Commands	**Command**	**Description**
	radius set qos cos	Sets the qos value sent by the RADIUS server as the cos value of the interface.

Platform Description	N/A

2.5 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 Examples	The following example extends RADIUS so as not to differentiate the IDs of private vendors: `Ruijie(config)# radius vendor-specific extend`	
Related Commands	**Command**	**Description**
	radius attribute	Configures vendor type.
	radius set qos cos	Sets the qos value sent by the RADIUS server as the cos value of the interface.
Platform Description	N/A	

2.6 radius-server account update retransmit

	Use this command to configure accounting update packet retransmission for the second generation 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 Mode	Global configuration mode	

Usage Guide	This command is used to configure accounting update packet retransmission for the second generation Web authentication user exclusively.
Configuration Examples	The following example configures accounting update packet retransmission for the second generation Web authentication user. `Ruijie(config)#radius-server account update retransmit`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.7 radius-server attribute 31

	Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute in global configuration mode. 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	**Command**	**Description**

Commands		
	radius-server host	Defines the RADIUS server.
Platform Description	N/A	

2.8 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 Description	**Parameter**	**Description**
	time *seconds*	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 *number*	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 Examples	The following example sets the timeout to 120 seconds and timeout times to 20. `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

		retransmission.
Platform Description	N/A	

2.9 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**
	minutes	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 1440 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 Examples	The following example sets the duration when the device stops sending requests to 1 minute. `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	

2.10 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**] { *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	oob authentication.
	ipv4-address	IPv6 address of the RADIUS security server host.
	ipv6-address	IPv4 address of the RADIUS security server host.
	auth-port *port-number*	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
	acct-port *port-number*	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
	test username *name*	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
	idle-time *time*	(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**] *text-string*	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 Description	N/A	

2.11 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**
	text-string	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 Examples	The following example defines the shared password **aaa** for the RADIUS security server: `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 Description	N/A

2.12 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**
	retries	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 Examples	The following example sets the number of retransmissions to 4: `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 Description	N/A	

2.13 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 Description	**Parameter**	**Description**
	port	The port number, in the range from 0 to 65,535.
Defaults	The default is a random number.	
Command Mode	Global configuration mode	
Usage Guide	The source port is random by default. This command is used to specify a source port.	
Configuration Examples	The following example configures source port 10000 to send RADIUS packets. `Ruijie(config)# radius-server source-port 10000`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

2.14 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**
	seconds	Timeout in the range from 1 to1,000 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 Examples	The following example sets the timeout to 10 seconds. `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 Description	N/A	

2.15 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	The default is DHCP 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 Description	N/A

2.16 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

2.17 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**
	ip-addr	Server IP address.
	Ipv6-addr	Server IPv6 address.
	port1	Server authentication port.
	port2	Server accounting port.

Defaults	No server is configured by default.
Command Mode	Server group configuration 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 Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

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 Examples	The following example displays RADIUS accounting statistics. `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 Description	N/A	

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 Examples	The following example displays RADIUS authentication statistics. `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 Examples	The following example displays RADIUS server group configuration. `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 Examples	The following example displays global RADIUS server parameters. `Ruijie# show radius parameter` `Server Timout:  5 Seconds` `Server Deadtime: 0 Minutes` `Server Retries:  3` `Server Dead Critera:` `Time:  10 Seconds` `Tries:  10`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

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/Global configuration mode/Interface configuration mode
Usage Guide	N/A
Configuration Examples	The following example displays the configuration of the RADIUS server. `Ruijie# show radius server` `erver 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 Description	N/A

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/Global configuration mode/Interface configuration mode
Usage Guide	N/A
Configuration Examples	The following example displays the configuration of the private vendors.

```
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-v 17 ersion 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-addre 79 ss 27 ipv4-multicast-addre 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 Description	N/A	

3 TACACS+ Commands

3.1 aaa group server tacacs+

	Use this command to group different TACACS+ server hosts. Use the **no** form of this command to remove the specified TACACS server group.
	aaa group server tacacs+ *group-name* **no aaa group server tacacs+** *group-name*

Parameter Description	**Parameter**	**Description**
	group_name	TACACS+ server group name. The group name 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 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**
	interface-name	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	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. This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer3 devices. If the specified interface is in a VRF instance, the route of this VRF instance is used for packet transmission.
Configuration Examples	The following example specifies the IP address of GigabitEthernet 0/0 for the outgoing TACACS+ packets. `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 Description	N/A

3.3 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**
	vrf_name	VRF name

Defaults	N/A
Command Mode	TACACS+ server group configuration 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 Examples	The following example specifies the VRF instance named vpn1 for the TACACS+ server group: `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 Description	N/A

3.4 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 Description	**Parameter**	**Description**
	ipv4-address	IPv4 address of the TACACS+ server.
	ipv6-address	IPv6 address of the TACACS+ server.

Defaults	No TACACS+ server is configured by default.
Command Mode	TACACS+ server group configuration 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	he 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 Description	N/A	

3.5 show tacacs

	Use this command to display the TACACS+ server configuration.
	show tacacs

Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the TACACS+ server configuration. `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	

3.6 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**] {*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
	ip-address	IP address of the TACACS+ host.
	ipv6-address	IPv6 address of the TACACS+ host.
	oob	Specifies an MGMT port as the source port for TACACS+ communication. The default is 49.
	port *integer*	Port number of the server. The range is from 1 to 65,535.
	timeout *integer*	Timeout time of TACACS+ host. The range is from 1 to 1,000.
	key *string*	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	

3.7 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**] *text-string*	
	no tacacs-server key	
Parameter Description	**Parameter**	**Description**
	text-string	Key string.
	0 | 7	Encryption type of key. 0 indicates no encryption; 7 indicates 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 Examples	The following example defines the authentication encryption key of TACACS+ server as aaa: `Ruijie(config)# tacacs-server key aaa`	
Related Commands	**Command**	**Description**
	tacacs-server host	Defines a TACACS+ host.
Platform Description	N/A	

3.8 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**
	seconds	Timeout interval. The range is from 1 to 1,000. The unit is second.
Defaults	The default timeout interval 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 Examples	The following example configures the timeout interval to 10 seconds: `Ruijie(config)# tacacs-server timeout 10`	
Related Commands	**Command**	**Description**
	tacacs-server host	Defines a TACACS+ secure server host.
Platform Description	N/A	

4 802.1X Commands

4.1 aaa authorization ip-auth-mode

	Use this command to set the IP authentication mode.	
	aaa authorization ip-auth-mode {disable | dhcp-server | radius-server | supplicant | mixed }	
Parameter Description	**Parameter**	**Description**
	disable	disable mode.
	dhcp-server	dhcp-server mode.
	radius-server	radius-server mode.
	supplicant	supplicant mode.
	mixed	Mixed mode
Defaults	The default is disabled mode	
Command Mode	Global configuration mode	
Usage Guide	Use the **show running-config** command to check the IP authentication mode.	
Configuration Examples	The following example sets the IP authentication mode to radius-server. `Ruijie# configure terminal` `Ruijie(config)# aaa new-model` `Ruijie(config)# aaa authorization ip-auth-mode radius-server` `Ruijie(config)# end` `Ruijie# show running-config` `!` `aaa new-model` `!` `aaa authorization ip-auth-mode radius-server` `!` `Ruijie# write memory`	
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 dot1x authentication users on the device.	
	clear dot1x user all	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear all the dot1x authentication users on the device.	
Configuration Examples	The following example clears all the dot1x authentication users: `Ruijie#clear dot1x user all`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.3 clear dot1x user id

	Use this command to clear the dot1x authentication user according to the user's session ID.	
	clear dot1x user id *session-id*	
Parameter Description	**Parameter**	**Description**
	session-id	The session ID of the dot1x authentication user.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear the dot1x authentication user according to the user's session ID.	
Configuration	The following example clears the dot1x authentication user whose session ID is 12345678.	

Examples	`Ruijie#clear dot1x user id 12345678`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.4 clear dot1x user mac

	Use this command to clear the dot1x authentication user according to the user's MAC address.	
	clear dot1x user mac *mac-addr*	
Parameter Description	**Parameter**	**Description**
	mac-addr	The MAC address of the dot1x authentication user.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear the dot1x authentication user according to the user's MAC address.	
Configuration Examples	The following example clears the dot1x authentication user whose MAC address is 0012.3456.789A. `Ruijie#clear dot1x user mac 0012.3456.789A`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.5 clear dot1x user name

	Use this command to clear the dot1x authentication user according to the username.	
	clear dot1x user mac *mac-addr*	
Parameter Description	**Parameter**	**Description**
	mac-addr	The username of the dot1x authentication user.

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to clear the dot1x authentication user according to the username,
Configuration Examples	The following example clears the dot1x authentication user named dot1x-user. `Ruijie#clear dot1x user name dot1x-user`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.6 dot1x accounting

	Use this command to configure the accounting list.
	dot1x accounting *list-name*

Parameter Description	**Parameter**	**Description**
	list-name	The name of the accounting list.

Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	If AAA does not adopts dot1x accounting as the default accounting method. Use this command to configure the dot1x 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 Description	N/A

4.7 dot1x auth-mode

	Use this command to specify the 802.1x authentication mode.	
	dot1x auth-mode { **eap** | **chap** | **pap** }	
	no dot1x auth-mode	
Parameter Description	**Parameter**	**Description**
	eap	Uses EAP-MD5 for authentication.
	chap	Uses CHAP for authentication.
	pap	Uses PAP for authentication.
Defaults	The default is eap mode.	
Command Mode	Global configuration mode	
Usage Guide	Use the **show dot1x** command to display the 802.1X configuration.	
Configuration Examples	The following example configures the eap authentication mode. `Ruijie(config)# dot1x auth-mode eap`	
Related Commands	**Command**	**Description**
	show dot1x	Displays the information about 802.1x.
Platform Description	N/A	

4.8 dot1x auth-address-table address

	Use this command to configure the authentication address table.	
	dot1x auth-address-table address *mac-addr* **interface** *interface*	
Parameter Description	**Parameter**	**Description**
	mac-addr	The MAC address of the authentication host.
	interface	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 Examples	The following example configures the authentication address table. `Ruijie(config)# dot1x auth-address-table 00d0.f800.0cb2 interface fastethernet 0/1`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

4.9 dot1x authentication

	Use this command to configure the authentication method list.
	dot1x authentication *list-name*
Parameter Description	**Parameter** / **Description** *list-name* / Authentication method list.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	If AAA does not adopt the default dot1x authentication, use this command to configure the dot1x authentication method.
Configuration Examples	The following example configures the authentication method list `Ruijie(config)# dot1x authentication dot1x-authen`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

4.10 dot1 authorization ip-auth-mode

	Use this command to enable interface IP authorization. **dot1x authorization ip-auth-mode** { **disable** | **supplicant** | **radius-server | dhcp-server | mixed** }

Parameter Description	Parameter	Description
	disable	Disables interface IP authorization.
	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	Interface IP authorization is disabled on interfaces by default.	
Command Mode	Interface 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. Interface IP authorization mode is prior to global configuration mode.	
Configuration Examples	The following example enables supplicant authorization mode. `Ruijie(config-if-GigabitEthernet 0/1)# dot1x authorization ip-auth-mode supplicant`	
Platform Description	N/A	

4.11 dot1x auto-req

	Use this command to configure 802.1X active authentication function in global configuration command. Use the **no** form of this command to restore the default setting.	
	dot1x auto-req	
	no dot1x auto-req	
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 actively initiate 802.1x authentication on the device. Use the **show dot1x auto-req** command to display the setting.	

Configuration Examples	The following example sets the device to automatically initiate 802.1x authentication. `Ruijie# configure terminal` `Ruijie(config)# dot1x auto-req` `Ruijie(config)# end` `Ruijie(config)# show dot1x auto-req` `Auto-Req: Enabled` `User-Detect : Enabled` `Packet-Num : 0` `Req-Interval: 30 Second`

Related Commands	**Command**	**Description**
	show dot1x auto-req	Displays the automatic authentication request information.

Platform Description	N/A

4.12 dot1x auto-req packet-num

	Use this command to set the number of authentication request messages that the device automatically sends. Use the **no** form of this command to restore the default setting.
	dot1x auto-req packet-num *num*
	no dot1x auto-req packet-num

Parameter Description	**Parameter**	**Description**
	num	Number of authentication request messages that the device sends automatically in the range from 0 to 1,000,000.

Defaults	The default is 0.
Command Mode	N/A
Usage Guide	Use the **show dot1x auto-req** command to display the setting.
Configuration Examples	The following example sets the device to automatically initiate 802.1x authentication continuously. `Ruijie# configure terminal` `Ruijie(config)# dot1x auto-req packet-num 0` `Ruijie(config)# end`

	Ruijie# show dot1x auto-req Auto-Req: Enabled User-Detect : Enabled Packet-Num : 0 Req-Interval: 30 Second
Related Commands	**Command** / **Description** **show dot1x auto-req** / Displays the authentication request information.
Platform Description	N/A

4.13 dot1x auto-req req-interval

	Use this command to set the interval of sending authentication request messages. Use the **no** form of this command to restore the default setting.
	dot1x auto-req req-interval *interval*
	no dot1x auto-req req-interval
Parameter Description	**Parameter** / **Description** *interval* / The time interval of actively sending authentication request messages by the device, in the range from 10 to 3600 in the unit of seconds.
Defaults	The default is 30 seconds.
Command Mode	Global configuration mode
Usage Guide	Use the **show dot1x auto-req** command to display the setting of this function.
Configuration Examples	The following example sets the time interval of sending authentication request message to 60 seconds. Ruijie# configure terminal Ruijie(config)# dot1x auto-req req-interval 60 Ruijie(config)# end Ruijie# show dot1x auto-req Auto-Req: Enabled User-Detect : Enabled

	Packet-Num : 0 Req-Interval: 60 Second

Related Commands	Command	Description
	show dot1x auto-req	Displays the authentication request information.

Platform Description	N/A

4.14 dot1x auto-req user-detect

	Use this command to configure active authentication detection to check whether the user is applying for 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 Description	Parameter	Description
	N/A	N/A

Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Use the **show dot1x auto-req** command to display the setting of this function.
Configuration Examples	The following example configures active authentication detection to check whether the user is applying for authentication. Ruijie# configure terminal Ruijie(config)# dot1x auto-req user-detect Ruijie(config)# end Ruijie# show dot1x auto-req Auto-Req: Enabled User-Detect : Enabled Packet-Num : 0 Req-Interval: 60 Second

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 the online probe function of the client. Use the **no** form of this command to restore the default setting.	
	dot1x client-probe enable	
	no do1x client-probe enable	
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 the online probe function of the client.	
Configuration Examples	The following example enables the online probe function of the client.	

```
Ruijie# configure terminal
Ruijie(config)# dot1x client-probe enable
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:  Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Enabled
Re-authen Period:   1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    10 sec
Supplicant Timeout:     10 sec
Server Timeout:     10 sec
Re-authen Max:  5 times
Maximum Request:    3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Enabled
```

	Eapol Tag Enable: Disabled Authorization Mode: Group Server

Related Commands	Command	Description
	show dot1x	Displays the 802.1x configurations.

Platform Description	N/A

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 Description	Parameter	Description
	N/A	N/A

Defaults	This functions is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	With the IAB function enabled on the port, if there is only RADIUS authentication method in the 802.1x authentication method list and all RADIUS servers in this method list take no effect, the switch will set the network accessing authority for users by the IAB method, and send the EAPOL-SUCCESS packets to the users. Except for the RADIUS authentication method, if there are other authentication methods in the 802.1x authentication method list, the IAB function will take no effect. (Such as the **aaa authentication dot1x default group radius none,** there exists none authentication method after the RADIUS authentication method. For the users of IAB authorized, as the user identity legality cannot be checked, no matter whether the accounting function is configured, they will not send the accounting request. With the AAA multi-domain authentication enabled globally, the 802.1x user authentication will not use the globally configured method list. After all RADIUS servers in the 802.1x globally configured method list are checked to be invalid, the IAB will directly send the successful authentication to the user with no need to enter the username, the AAA multi-domain authentication on this port is useless.
Configuration Examples	The following example enables the server IAB (Inaccessible Authentication Bypass) function on the port.

	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface fa 0/10 Ruijie(config-if)# dot1x port-control auto Ruijie(config-if)# dot1x critical Ruijie(config-if)# end

Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

4.17 dot1x critical recovery action reinitialize

	Use this command to handle the all users that have passed the inaccessible authentication bypass on the port after the RADIUS server returns to normal. Use the **no** form of this command to restore the default setting.
	dot1x critical recovery action reinitialize
	no dot1x critical recovery action reinitialize

Parameter Description	Parameter	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 handles the all users that have passed the inaccessible authentication bypass on the port after the RADIUS server returns to normal. Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface fa 0/10 Ruijie(config-if)# dot1x port-control auto

	`Ruijie(config-if)# dot1x critical recovery action reinitialize` `Ruijie(config-if)# end`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.18 dot1x dbg-filter

	Use this command to print the debug information of the device with the 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**
	H.H.H	The MAC address of the 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 Description	N/A

4.19 dot1x default-user-limit

	Use this command to set the maximum number of authentication users on controlled interface. Use the **no** form of this command to restore the default setting.
	dot1x default-user-limit *num*

	no dot1x default-user-limit	
Parameter Description	**Parameter**	**Description**
	num	The maximum number of authentication users allowed by a controlled interface, in the range from 1 to 1,000,000.
Defaults	The default is 1,000,000.	
Command Mode	Interface configuration mode	
Usage Guide	Use the **show dot1x dynamic-vlan** command to display the 802.1x setting.	
Configuration Examples	The following example sets the maximum number of authentication users on a controlled interface. `Ruijie# configure terminal` `Ruijie(config)# interface fa 0/10` `Ruijie(config-if)# dot1x default-user-limit 1000` `Ruijie(config)# end` `Ruijie#`	
Related Commands	**Command**	**Description**
	show dot1x port-control interface fastEthernet 0/10	Displays the number of users allowed by a specific 802.1x interface.
	show dot1x port-control interface fastEthernet 0/10	Displays the number of users allowed by a specific 802.1x interface.
Platform Description		

4.20 dot1x default

	Use this command to restore 802.1X configuration to the default setting.	
	dot1x default	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	

Usage Guide	Use the **show dot1x** command to display the 802.1X configuration.
Configuration Examples	The following example restore 802.1X configuration to the default setting. `Ruijie# configure terminal` `Ruijie(config)# dot1x default` `Ruijie(config)# end` `Ruijie# end`
Related Commands	**Command** / **Description** **show dot1x** / Displays the 802.1X information .
Platform Description	N/A

4.21 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 Description	**Parameter** / **Description** N/A / N/A
Defaults	This function is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Use the **show dot1x port-control interface** command to display the configuration.
Configuration Examples	The following example configures single MAB authentication. `Ruijie# configure terminal` `Ruijie(config)# interface fa 0/1` `Ruijie(config)# dot1x mac-auth-bypass` `Ruijie(config)# end` `Ruijie#`
Related	**Command** / **Description**

Commands	**show dot1x port-control interface**	Displays the information about 802.1x on the interface .
Platform Description	N/A	

4.22 dot1x mac-auth-bypass multi-user

	Use this command to configure multiple MAB authentication, 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 Description	**Parameter**	**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 Examples	The following example configures multiple MAB authentication. `Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass multi-user`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.23 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 Description	**Parameter**	**Description**
	time	The online time, in the range from1 to 65,535 in the unit of seconds.
Defaults	The default is 0 second.	

Command Mode	Interface configuration mode
Usage Guide	Use the **show run** command to display the 802.1X configuration.
Configuration Examples	The following example sets the MAB authentication timeout interval. `Ruijie# configure terminal` `Ruijie(config)# interface fa0/1` `Ruijie(config)# dot1x mac-auth-bypass timeout-activity` `Ruijie(config)# end` `Ruijie#write`

Related Commands	**Command**	**Description**
	show dot1x port-control interface	Displays the information about 802.1x on the interface.
	show dot1x port-control interface	Displays the information about 802.1x on the interface.
Platform Description	N/A	

4.24 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 Description	**Parameter**	**Description**
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use the **show run** command to display the 802.1X configuration.	

Configuration Examples	The following example configures the MAB violation. `Ruijie# configure terminal` `Ruijie(config)# interface fa0/1` `Ruijie(config)# dot1x mac-auth-bypass violation` `Ruijie(config)# end` `Ruijie#write`

Related Commands	**Command**	**Description**
	show dot1x port-control interface	Displays the information about 802.1x on the interface.

Platform Description	N/A

4.25 dot1x mac-auth-bypass vlan

	Use this command to configure the MAB VLAN function. Use the **no** form of this command to restore the default setting.
	dot1x mac-auth-bypass vlan *vlan-list*
	no dot1x mac-auth-bypass vlan *vlan-list*

Parameter Description	**Parameter**	**Description**
	vlan-list	Configures the MAB VLANs.

Defaults	This function is disabled by default.
Command Mode	Interface configuration mode.
Usage Guide	Use this command to allow users within specified VLANs on the port to perform MAB authentication.
Configuration Examples	The following example configures MAB VLANs. `Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass vlan 5, 8-20`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.26 dot1x max-req

	During interaction between the dot1x and the server, the dot1x will send a request to the server again if it does not receive a response from the server within a certain period of time. Use this command to set the maximum number of authentication requests sent to the server. Use the **no** form of this command to restore the default setting.	
	dot1x max-req *count*	
	no dot1x max-req	
Parameter Description	**Parameter**	**Description**
	count	Maximum number of authentication requests sent to the server in the range 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 Examples	The following example sets the maximum number of authentication requests to 7. `Ruijie# configure terminal` `Ruijie(config)# dot1x max-req 7` `Ruijie(config)# end` `Ruijie#`	
Related Commands	**Command**	**Description**
	show dot1x	Displays the information about 802.1x.
Platform Description	N/A	

4.27 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 Description	**Parameter**	**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

4.28 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 Description	**Parameter**	**Description**
	time	Sets the quiet period after the multiple MAB authentication failure, in the range from 0 to 65535 in the unit of seconds,

Defaults	The default is 0, 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	

4.29 dot1x port-control auto

	Use this command to configure the 802.1x authentication on the port. Use the **no** form of this command to restore the default setting.	
	dot1x port-control auto	
	no dot1x port-control	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use the **show dot1x** command to display the 802.1X configuration.	
Configuration Examples	`The following example configures the 802.1x authentication on the port. Ruijie# configure terminal` `Ruijie(config)# interface g0/1` `Ruijie(config-if)# dot1x port-control auto` `Ruijie(config-if)# end` `Ruijie#`	
Related Commands	**Command**	**Description**
	show dot1x	Displays the information about 802.1X.
Platform Description	N/A	

4.30 dot1x probe-timer interval

	Use this command to set the Ruijie terminal detection interval.	
	dot1x probe-timer interval *time*	
Parameter Description	**Parameter**	**Description**
	time	Terminal detection interval in the range from 1 to 65,535 in the unit of seconds.

Defaults	The default is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	The default setting is recommended.
Configuration Examples	The following example sets Ruijie terminal detection interval to 30 seconds. `Ruijie(config)# dot1x probe-timer interval 30`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.31 dot1x probe-timer alive

	Use this command to set the Ruijie terminal alive interval.
	dot1x probe-timer alive *time*

Parameter Description	**Parameter**	**Description**
	time	Terminal alive interval, 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	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 Examples	The following example sets Ruijie terminal alive interval to 120 seconds. `Ruijie(config)# dot1x probe-timer alive 120`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.32 dot1x private-supplicant-only

	Use this command to filter non-Ruijie client. 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 Mode	Global configuration mode
Usage Guide	You can use the **show dot1x private-supplicant-only** command to check the 802.1x setting.
Configuration Examples	The following example filters non-Ruijie client. `Ruijie# configure t` `Ruijie(config)# dot1x private-supplicant-only` `Ruijie(config)# end` `Ruijie#`

Related Commands	**Command**	**Description**
	show dot1x private-supplicant-only	Displays the information about the private supplicant.

Platform Description	N/A

4.33 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`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.34 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 Description	**Parameter**	**Description**
	N/A	N/A

Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Redirect to the supplicant software download website through the browser. See *Web Authentication Configuration Guide* for details about parameters.
Configuration Examples	The following example enables the second generation su upgrade function, `Ruijie(config)# dot1x redirect`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

4.35 dot1x reauth-max

	Use this command to set the maximum number of supplicant re-authentication. Use the **no** form of this command to restore the default setting.	
	dot1x reauth-max *count*	
	no dot1x reauth-max	
Parameter Description	**Parameter**	**Description**
	count	Maximum number of re-authentication in the range from 1 to 10
Defaults	The default s 3.	
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 Examples	The following example sets the maximum number of re-authentication to 5.	

```
Ruijie# configure terminal
Ruijie(config)# dot1x reauth-max 5
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:  Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Enable
Re-authen Period:   1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    10 sec
Supplicant Timeout:     10 sec
Server Timeout:     10 sec
Re-authen Max:  5 times
Maximum Request:    3 times
```

	Filter Non-RG Supp: Disabled Client Oline Probe: Disabled Eapol Tag Enable: Disabled Authorization Mode: Group Server
Related Commands	**Command** / **Description** **show dot1x** / Displays the information about 802.1x.
Platform Description	N/A

4.36 dot1x re-authentication

	Use this command to enable the 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	The default setting is recommended.
Configuration Examples	The following example enables the re-authentication function, Ruijie# configure terminal Ruijie(config)# dot1x re-authentication Ruijie(config)# end Ruijie# show dot1x 802.1X Status: Enabled Authentication mode: EAP-MD5 Authed User Number: 0 Re-authen Enabled: Enabled Re-authen Period: 1000 sec Quiet Timer Period: 1000 sec

	Tx Timer Period: 10 sec Supplicant Timeout: 10 sec Server Timeout: 10 sec Re-authen Max: 3 times Maximum Request: 3 times Filter Non-RG Supp: Disabled Client Oline Probe: Disabled Eapol Tag Enable: Disabled Authorization Mode: Group Server

Related Commands	Command	Description
	show dot1x	Displays the information about 802.1X.

Platform Description	N/A

4.37 dot1x timeout re-authperiod

	Use this command to set the re-authentication interval when re-authentication is enabled. Use the **no** form of this command to restore the default setting.
	dot1x timeout re-authperiod *time*
	no dot1x timeout re-authperiod

Parameter Description	Parameter	Description
	time	Authentication interval, in the range from 1 to 65,535 in the unit of seconds.

Defaults	The default is 3600 seconds.
Command Mode	Global configuration mode
Usage Guide	Use the **show dot1x** command to display the 802.1X configuration.
Configuration Examples	The following example sets the re-authentication interval to 1000 seconds. Ruijie# configure terminal Ruijie(config)# dot1x timeout re-authperiod 1000 Ruijie(config)# end Ruijie# show dot1x

	802.1X Status: Enabled Authentication mode EAP-MD5 Authed User Number: 0 Re-authen Enabled: Disabled Re-authen Period: 1000 sec Quiet Timer Period: 1000 sec Tx Timer Period: 3 sec Supplicant Timeout: 3 sec Server Timeout: 5 sec Re-authen Max: 3 times Maximum Request: 3 times Filter Non-RG Supp: Disabled Client Oline Probe: Disabled Eapol Tag Enable: Disabled Authorization Mode: Group Server

Related Commands	Command	Description
	show dot1x	Displays the information about 802.1X.
Platform Description	N/A	

4.38 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**
	time	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 Examples	The following example sets the quiet period after authentication failure to 1000 seconds. `Ruijie# configure terminal` `Ruijie(config)# dot1x timeout quiet-period 1000` `Ruijie(config)# end` `Ruijie# show dot1x` `802.1X Status: Enabled` `Authentication mode: EAP-MD5` `Authed User Number: 0` `Re-authen Enabled: Disabled` `Re-authen Period: 3600 sec` `Quiet Timer Period: 1000 sec` `Tx Timer Period: 3 sec` `Supplicant Timeout: 3 sec` `Server Timeout: 5 sec` `Re-authen Max: 3 times` `Maximum Request: 3 times` `Filter Non-RG Supp: Disabled` `Client Oline Probe: Disabled` `Eapol Tag Enable: Disabled` `Authorization Mode: Group Server`

Related Commands	**Command**	**Description**
	show dot1x	Displays the information about 802.1X.

Platform Description	N/A

4.39 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 Description	**Parameter**	**Description**
	time	Authentication timeout between the device and the supplicant

		The range is from 1 to 65,535 seconds.
Defaults	The default is 3 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Use the **show dot1x** command to show display 802.1X configuration.	
Configuration Examples	The following example sets the authentication timeout between the device and the supplicant to 10s: `Ruijie# configure terminal` `Ruijie(config)# dot1x timeout supp-timeout 10` `Ruijie(config)# end` `Ruijie# show dot1x` `802.1X Status: Enabled` `Authentication Mode: EAP-MD5` `Authed User Number: 0` `Re-authen Enabled: Disabled` `Re-authen Period: 1000 sec` `Quiet Timer Period: 1000 sec` `Tx Timer Period: 3 sec` `Supplicant Timeout: 10 sec` `Server Timeout: 10 sec` `Re-authen Max: 3 times` `Maximum Request: 3 times` `Filter Non-RG Supp: Disabled` `Client Oline Probe: Disabled` `Eapol Tag Enable: Disabled` `Authorization Mode: Group Server`	
Related Commands	**Command**	**Description**
	show dot1x	Show Displays the information about 802.1x.
Platform Description	N/A	

4.40 dot1x timeout server-timeout

	Use this command to set the server timeout interval. Use the **no** form of this command to restore the default setting	
	dot1x timeout server-timeout *time*	
	no dot1x timeout server-timeout	
Parameter Description	**Parameter**	**Description**
	time	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	Use the **show dot1x** command to display 802.1X configuration.	
Configuration Examples	The following example set the server timeout interval to 10 seconds.	

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout server-timeout 10
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:  Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Disabled
Re-authen Period:   1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    3 sec
Supplicant Timeout:     3 sec
Server Timeout:     10 sec
Re-authen Max:  3 times
Maximum Request:    3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:   Disabled
```

	`Authorization Mode: Group Server`

Related Commands	Command	Description
	show dot1x	Displays the information about 802.1x.

Platform Description	N/A

4.41 dot1x timeout tx-period

	Use this command to set the request/id packet retransmission interval. Use the **no** form of this command to restore the default setting.
	dot1x timeout tx-period *time*
	no dot1x timeout tx-period

Parameter Description	Parameter	Description
	time	The request/id packet retransmission interval, in range from 1 to 65,535 in the unit of seconds.

Defaults	The default is 3 seconds.
Command Mode	Global configuration mode
Usage Guide	Use the **show dot1x** command to display 802.1X configuration.
Configuration Examples	The following example sets the request/id packet retransmission interval to 10 seconds.

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout tx-period 10
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:  Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Disabled
Re-authen Period:   1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    10 sec
Supplicant Timeout:     10 sec
```

	Server Timeout: 10 sec Re-authen Max: 3 times Maximum Request: 3 times Filter Non-RG Supp: Disabled Client Oline Probe: Disabled Eapol Tag Enable: Disabled Authorization Mode: Group Server
Related Commands	**Command** / **Description** **show dot1x** / Displays the information about 802.1X.
Platform Description	N/A

4.42 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 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 accounting only when users obtain valid IP addresses.
Configuration Examples	The following example enables IP address-triggered accounting. `Ruijie(config)#dot1x valid-ip-acct enable`
Platform Description	N/A

4.43 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 Description	**Parameter**	**Description**
	time	IP address-triggered accounting timeout in the unit of minutes

Defaults	The default is 5 minutes.
Command Mode	Global configuration 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 Examples	The following example configures IP address-triggered accounting timeout. `Ruijie(config)# dot1x valid-ip-acct timeout 10`
Platform Description	N/A

4.44 show dot1x

	Use this command to display the 802.1x setting.
	show dot1x

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 802.1x setting. `Ruijie# show dot1x` `802.1X Status: Enabled` `Authentication Mode: EAP-MD5` `Authed User Number: 0`

	Re-authen Enabled: Disabled Re-authen Period: 3600 sec Quiet Timer Period: 10 sec Tx Timer Period: 3 sec Supplicant Timeout: 3 sec Server Timeout: 5 sec Re-authen Max: 3 times Maximum Request: 3 times Filter Non-RG Supp: Disabled Client Oline Probe: Disabled Eapol Tag Enable: Disabled Authorization Mode: Group Server Ruijie#

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request retransmissions.
	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 retransmission interval.
Platform Description	N/A	

4.45 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 Description	Parameter	Description
	addr	Physical IP address that can be authenticated

	interface	Interface 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 the 802.1x authentication address table: `Ruijie# show dot1x auth-address-table` `interface:g3/1` `----------` `mac-addr 00D0.F800.0001` `Ruijie#`	
Related Commands	**Command**	**Description**
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request retransmissions.
	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 retransmission interval.
Platform Description	N/A	

4.46 show dot1x auto-req

	Use this command to display the active authentication status and parameters.	
	show dot1x auto-req	
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 active authentication status and parameters. `Ruijie# show dot1x auto-req` `Auto-Req: Disabled` `User-Detect : Enabled` `Packet-Num : 0` `Req-Interval: 30 Seconds` `Ruijie#`

Related Commands	**Command**	**Description**
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request retransmissions.
	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 retransmission interval.

Platform Description	N/A

4.47 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: 2 times` `Ruijie#`	
Related Commands	**Command**	**Description**
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request retransmissions.
	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 retransmission interval.
Platform Description	N/A	

4.48 show dot1x port-control

	Use this command to display the information about ports that participate in authentication.	
	show dot1x port-control [**interface** *interface-type interface-number*]	
Parameter Description	**Parameter**	**Description**
	interface-type	Interface type
	*interface-numbe*r	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 information about ports that participate in the authentication. `Ruijie# show dot1x port-control` `Interface Mode Dynamic-User Static-User Max-User Authened Mab` `--------- ---------- ------------ ----------- -------- -------- ---------` `Fa0/5 mac-based 0 1 6000 yes` `disable` `Ruijie#`

Related Commands	**Command**	**Description**
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request retransmissions**.**
	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 retransmission interval.

Platform Description	N/A

4.49 show dot1x private-supplicant-only

	Use this command to display the information about the private supplicant.
	show dot1x private-supplicant-only

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 information about the private supplicant: `Ruijie# show dot1x private-supplicant-only` `private-supplicant-only:: disabled` `Ruijie#`

Related Commands	**Command**	**Description**
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request retransmissions.
	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 retransmission interval.

Platform Description	N/A

4.50 show dot1x probe-timer

	Use this command to display the online probing configurations.
	show dot1x probe-timer

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 online probing configuration. `Ruijie# show dot1x probe-timer` `Hello Interval: 20 Seconds` `Hello Alive: 250 Seconds` `Ruijie#`
Related Commands	**Command** / **Description** Hello Interval / Sets the probe period. Hello Alive / Sets the probe alive interval**.**
Platform Description	N/A

4.51 show dot1x re-authentication

	Use this command to display re-authentication status.
	show dot1x re-authentication
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 re-authentication status. `Ruijie# show dot1x re-authentication` `eauth-enabled: disabled` `Ruijie#`
Related	**Command** / **Description**

Commands	Reauth-Enabled	Whether to enable re-authentication.
Platform Description	N/A	

4.52 show dot1x reauth-max

	Use this command to display the maximum number of re-authentication.	
	show dot1x reauth-max	
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 maximum number of re-authentications: `Ruijie# show dot1x reauth-max` `reauth-max: 2 times` `Ruijie#`	
Related Commands	**Command**	**Description**
	Reauth-Max	Sets the maximum number of re-authentication.
Platform Description	N/A	

4.53 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 Examples	The following example displays the summary of 802.1x authentication.

```
Ruijie(config)#sh dot1x summary

ID       Username   MAC           Interface VLAN Auth-State
Backend-State Port-Status User-Type Time

--------- ---------- --------------  --------- ---- ---------------
------------ ----------- --------- ------------------

16777228  6c626dd... 6c62.6dd5.84ac  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777229  6c626dd... 6c62.6dd5.84b4  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777217  0023aea... 0023.aeaa.4286  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m32s

16777227  6c626dd... 6c62.6dd5.84af  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777218  6c626dd... 6c62.6dd5.84aa  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777219  6c626dd... 6c62.6dd5.84b2  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777230  6c626dd... 6c62.6dd5.84ad  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777223  6c626dd... 6c62.6dd5.84b0  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777222  6c626dd... 6c62.6dd5.84a8  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777220  6c626dd... 6c62.6dd5.84ab  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777221  6c626dd... 6c62.6dd5.84b3  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777226  6c626dd... 6c62.6dd5.84ae  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777225  6c626dd... 6c62.6dd5.84b1  Gi0/5    2   Authenticated   Idle
Authed     static   0days 0h 0m 2s

16777224  6c626dd... 6c62.6dd5.84a9  Gi0/5    2   Authenticated   Idle
```

```
Authed     static   0days 0h 0m 2s

Ruijie(config)#show dot1x u

Ruijie(config)#show dot1x user i

Ruijie(config)#show dot1x user id 16777226


User name: 6c626dd584ae

User id: 16777226

Type: static

Mac address is 6c62.6dd5.84ae

Vlan id is 2

Access from port Gi0/5

Time online: 0days 0h 3m55s

Max user number on this port is 0

No accounting

Permit proxy user

Permit dial user

IP privilege is 0

 user acl-name 6c626dd584ae_6_0_0 :


Ruijie(config)#show dot1x user mac 6c62.6dd5.84a9


User name: 6c626dd584a9

User id: 16777224

Type: static

Mac address is 6c62.6dd5.84a9

Vlan id is 2

Access from port Gi0/5

Time online: 0days 0h 4m 7s

Max user number on this port is 0

No accounting

Permit proxy user

Permit dial user

IP privilege is 0

 user acl-name 6c626dd584a9_6_0_0 :
```

```
Ruijie(config)#show dot1x user name 6c626dd584a9

User name: 6c626dd584a9
User id: 16777224
Type: static
Mac address is 6c62.6dd5.84a9
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 4m19s
Max user number on this port is 0
No accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name 6c626dd584a9_6_0_0 :
```

Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request retransmissions**.**
	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 retransmission interval.

Platform Description	N/A

4.54 show dot1x timeout quiet-period

	Use this command to display the quite period after the authentication failure.
	show dot1x timeout quiet-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 quiet period after the authentication failure.
Configuration Examples	The following example displays the quiet period after the authentication failure. `Ruijie#show dot1x timeout quiet-period` `Quiet-Period: 10 Seconds` **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 Description	N/A

4.55 show dot1x timeout re-authperiod

	Use this command to display the re-authentication interval.
	show dot1x timeout re-authperiod
Parameter Description	**Parameter** / **Description** N/A / N/A
Defaults	N/A
Command	Privileged EXEC mode/ Global configuration mode/ Interface configuration mode

Mode	
Usage Guide	Use this command to display the re-authentication interval.
Configuration Examples	The following example displays the re-authentication interval.: `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 Description	N/A

4.56 show dot1x timeout server-timeout

	Use this command to display the server timeout interval.
	show dot1x timeout server-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 server timeout interval.
Configuration Examples	Use this command to display the server timeout interval. `Ruijie#show dot1x timeout server-timeout` `Server-Timeout: 5 Seconds` **Parameter** / **Description** Server-Period / Server timeout interval.

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.57 show dot1x timeout supp-timeout

	Use this command to display the request/challenge packet 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 packet re-transmission interval.	

Configuration Examples

Use this command to display the request/challenge packet re-transmission interval:

```
Ruijie#show dot1x timeout supp-timeout


Supp-Timeout: 3 Seconds
```

Parameter	Description
Server-Period	The request/challenge packet re-transmission interval.

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.58 show dot1x timeout tx-period

	Use this command to display the request/id packet 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 packet re-transmission interval.	
Configuration Examples	Use this command to display the request/ id packet re-transmission interval: `Ruijie#show dot1x timeout tx-period` `Tx-Period: 30 Seconds` **Parameter** / **Description** Tx-Period / Request/id packet re-transmission interval.	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.59 show dot1x user id

	Use this command to display the information about the 802.1X authentication user according to the user ID.	
	show dot1x user id *id*	
Parameter Description	**Parameter**	**Description**
	id	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 summary, Memorize the user ID hat you want to check. Use this command to display the detailed user information according to the user 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.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 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 Description	N/A

4.60 show dot1x user mac

	Use this command to display the information about the 802.1X authentication user according to the user's MAC address.
	show dot1x user mac *mac-addr*
Parameter Description	**Parameter** / **Description** *mac-addr* / User's 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 the 802.1X authentication summary, Memorize the MAC address of the user that you want to check. Use this command to display the detailed user information according to the user's MAC address.
Configuration Examples	The following example displays the information about the 802.1X authentication user according to the the user's MAC address.

```
Ruijie#show dot1x user mac 0023.aeaa.4286


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 Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

4.61 show dot1x user name

	Use this command to display the information about the 802.1X authentication user according to the username.	
	show dot1x user name *name*	
Parameter Description	**Parameter**	**Description**
	name	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 the 802.1X authentication summary, Memorize the user name that you to check. And use this command to display the detailed user information according to the user name.
Configuration Examples	The following example displays the information about the 802.1X authentication user according to the user name.

```
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 Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

5 Web Authentication Commands

5.1 accounting

	Use this command to set the 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**
	method-list	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**

	method-list	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 the Web authentication method list configured in AAA. The first generation authentication does not support the authentication method list configuration.	
Configuration Examples	The following example sets the **mlist1** authentication method for the **eportalv2** template. `Ruijie# clear web-auth direct-site`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

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 Examples	The following example adopts the IP only mode for the **eportalv2** template. `Ruijie(config.tmplt.eportalv2)# bindmode ip-only-mode`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

5.4 clear web-auth user

	Use this command to force the user to go offline.
	clear web-auth user { **all | ip** *ip-address* | **mac** *mac-address* **| name** *name-string* | **session-id** *num* }
Parameter Description	**Parameter** / **Description**
	ip-address / Specifies the user's IPv4 address.
	mac-address / Specifies the user's MAC address.
	name-string / Specifies the user name.
	num / Specifies the user's AAA session ID.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	The following example forces all users to go offline. `Ruijie# clear web-auth user all`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

5.5 clear web-auth direct host

	Use this command to clear all authentication-exempted users.	
	clear web-auth direct-host	
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 Description	N/A	

5.6 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 Examples	The following example clears all authentication-exempted network resources. `Ruijie# clear web-auth direct-site`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

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**
	ip-address	IPv4 address.
	ip-mask	(Optional) IPv4 mask.

Defaults	No authentication-exempted ARP resource is configured by default.
Command Mode	Privileged EXEC 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 Examples	The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource. `Ruijie(config)# http redirect direct-arp 172.16.0.1`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

5.8 http redirect direct-site

	Use this command to set the range of authentication-exempted network resource. Use the **no** form of this command to restore the default setting.
	http redirect direct-site { *ip-address* [*ip-mask*] [**arp**] }
	no http redirect direct-site { *ip-address* [*ip-mask*] }

Parameter Description	**Parameter**	**Description**
	ip-address	IPv4 address of the network resource free of authentication.
	ip-mask	IPv4 address mask of the network resource free of authentication (optional)
	arp	If the ARP CHECK is enabled on the access device, the keyword arp is needed for ARP binding of the network resources free of authentication (optional). It is necessary for IPv4 network resources only.

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 Web sites free of authentication. Up to 50 network resource ranges can be free of authentication.
Configuration Examples	The following example sets the Web site with the IP address 172.16.0.1 as the authentication-exempted resource. `Ruijie(config)# http redirect direct-site 172.16.0.1`

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**
	port-num	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 Examples	The following example redirects users' HTTP requests with port 8080. `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 recover the maximum number of HTTP sessions that can be originated by an unauthenticated user to 3.
	http redirect session-limit *session-num* [**port** *port-session-num*]
	no http redirect *session-limit*

Parameter Description	**Parameter**	**Description**
	session-num	Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255.
	port-session-num	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**
	seconds	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. `Ruijie(config)# http redirect timeout 4`	
Related Commands	**Command**	**Description**
	show http redirect	Displays the HTTP redirection configuration.
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**
	ip-address	The IPv4 address of the portal server.
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	The following example sets the IP address of the eportalv1 template to 172.16.0.1..	

Examples	`Ruijie(config.tmplt.eportalv1)#ip 172.16.0.1` `Ruijie(config.tmplt.eportalv1)#`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

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**
	interface-type	Port type
	interface-num	Port No.

Defaults	No communication interface is specified by default.
Command Mode	Global configuration mode
Usage Guide	N/A
Configuration Examples	The following example specifies an aggregate port as the communication port. `Ruijie (config)# ip portal source-interface Aggregateport 1`
Platform Description	N/A

5.14 port

	Use this command to set a communication 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**
	port	The communication port of the portal server, which is on only the second 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 communication port number of the eportalv2 server to 10000. `Ruijie(config.tmplt.eportalv2)#port 10000`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

5.15 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 Mode	Privileged EXEC 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 Description	N/A

5.16 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	I N/A

Configuration Examples

The following example displays the address range of the authentication-exempted ARP.

```
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

5.17 show web-auth direct-host

	This command is used to display the Web authentication-exempted users.
	show web-auth direct-host

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 Web authentication-exempted users.

```
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

5.18 show web-auth direct-site

	Use this command to display the range of the Web authentication-exempted network resource.
	show web-auth direct-site

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.

```
Ruijie(config)#show web-auth direct-site

Direct sites:

  Address        Mask           ARP Binding

  ---------------  ---------------  -----------

  1.1.1.1        255.255.255.255 Off

  2.2.2.2        255.255.255.255 On
```

	Ruijie(config)# Field / Description Address / IP address. Mask / IP mask. ARP Binding / Displays whether the ARP binding function is enabled.
Platform Description	N/A

5.19 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 Examples	The following example displays the HTTP redirect configuration `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	

5.20 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 Examples	The following example displays the TCP interception port. `Ruijie#show web-auth rdport` `Rd-Port:` `80` `Ruijie#`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

5.21 show web-auth template

	Use this command to display the portal server configuration.	
	show web-auth template	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the portal server configuration.
Configuration Examples	The following example displays the port server configuration.

```
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 and the intra portal server intra.
Port	The protocol packet communication port of the server, which is on only the second generation portal server.
Acctmlist	Accounting method list name, which is on only the second generation portal server and the intra portal server.

	Authmlist	Authentication method list name. which is on only the second generation portal server and the intra portal server.
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

5.22 show web-auth user

	Use this command 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-string* | **session-id** *num* }	
Parameter Description	**Parameter**	**Description**
	ip-address	IPv4 address of the user.
	mac-address	MAC address of the user.
	name-string	User name.
	num	AAA session ID.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the global Web authentication configuration and statistics.	

```
Ruijie# show web-auth user

  Current user num  :  4


Address          Online   Time Limit     Time Used    Status

---------------- -------  ------------- -------------- --------

192.168.0.11      On       0d 01:00:00    0d 00:15:10     Active

192.168.0.13      On       0              0d 00:00:59     Active

192.168.0.25      Off      0              0               Create

192.168.0.46      Off      0d 01:00:00    0d 01:00:00     Destroy
```

```
Ruijie# show web-auth user 192.168.0.11
Address      :   192.168.0.11
 Mac          :   00d0.f800.2233
 Port         :   Fa0/2
 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

5.23 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
	url-string	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 Examples	The following example sets the eportalv1 template URL to **http://www.web-auth.net/login**. `Ruijie(config.tmplt.eportalv1)#url http://www.web-auth.net/login`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

5.24 web-auth dhcp-check

	Use this command to enable DHCP IP address check. Use **no** form of this command to restore the default setting.
	web-auth dhcp-check
	no web-auth dhcp-check

Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	DHCP IP address check is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Only users whose IP addresses are allocated by DHCP are allowed to take authentication.	
Configuration Examples	The following example enables DHCP IP address check. `Ruijie (config)# web-auth dhcp-check`	

Platform Description	N/A

5.25 web-auth direct-host

	Use this command to set the authentication-exempted IP address range. Use the **no** form of this command to restore the default setting.	
	web-auth direct-host *ip-address [ip-mask*] [**port** *interface-name]* [**arp**]	
	no web-auth direct-host { *ip-address* [i*p-mask*] }	
Parameter Description	**Parameter**	**Description**
	ip-address	IPv4 address free of authentication
	ip-mask	Mask of the IPv4 address free of authentication (optional).
	port *interface-name*	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.
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`	
Related Commands	**Command**	**Description**
	show web-auth direct-host	Displays the users free of Web authentication.
Platform Description	N/A	

5.26 web-auth enable

	Use this command to enable the Web authentication function on the 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 [**eportalv1 | eportalv2 |** *template-name*]
	no web-auth enable

Parameter Description	**Parameter**	**Description**
	eportalv1	Applies the first generation authentication template.
	eportalv2	Applies the second generation authentication template.
	template-name	Customized template.

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. `Ruijie(config)# interface GigabitEthernet 0/14` `Ruijie(config-if-GigabitEthernet 0/14)# web-auth enable`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

5.27 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**
	num / 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

5.28 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**
	key-string / 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 Description	N/A	

5.29 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 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.
	template-name	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 Examples	The following example configures the **eportalv1** template. `Ruijie(config)# web-auth template eportalv1` `Ruijie(config.tmplt.eportalv1)#`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

5.30 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	The access device maintains the online user information (including online duration) and updates it at certain interval, to monitor the network resource used by online users. This command is used to change the interval at which the online user information is updated.
Configuration Examples	The following example sets the interval at which the online user information is updated to 30 seconds. `Ruijie(config)# web-auth update-interval 30`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

6 SCC Commands

6.1 Identifier Description

The following is a list of command identifiers used in commands for reference:

Identifier	Description
vlanlist	Authentication-exemption VLAN list
interval	Authenticated-user online-status detection interval
thredshold	The traffic threshold of authenticated-user online-status detection

6.2 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**
	vlanlist	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	
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`	
Platform Description	This command is supported only on switches.	

6.3 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**
	max-user-num	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
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`
Platform Description	This command is supported only on switches.

6.4 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**
	interval	Indicates the interval of traffic detection (in minutes). The range is from 6 to 65,535 in minutes on a non-switch device or from 6 to 65,535 in minutes on a switch.
	threshold	Indicates the traffic threshold (in bytes). The range is from 0 to

		4,294,967,294 in bytes. The value of 0 indicates that the user is disconnected when no traffic of the user is detected.
Defaults	By default, the detection interval is 8 hours and the traffic threshold is 0.	
Command Mode	Global configuration mode	
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`	
Platform Description	N/A	

6.5 show direct-vlan

	Use this command to display the authentication-exemption VLAN configuration. **show direct-vlan**	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the authentication-exemption VLAN configuration. `Ruijie #show direct-vlan` `direct-vlan 5,7,100`	
Platform Description	N/A	

6.6 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**
	interface-name / Interface name
Command Mode	Privileged EXEC mode
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`
Platform Description	N/A

6.7 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

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`
Platform Description	N/A

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* }	
Parameter Description	**Parameter**	**Description**
	ip-address	IPv4 address to be bound
	ipv6-address	IPv6 address to be bound
	mac-address	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 Description	**Parameter**	**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. `Ruijie(config)# address-bind 3.3.3.3 00d0.f811.1112` `Ruijie(config)# address-bind install`	
Related Commands	**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	**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. `Ruijie# configure terminal` `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 Description	N/A

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 Description	**Parameter** / **Description** *interface-id* / 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 Examples	The following example configures the exception port. `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 Description	N/A

7.5 show address-bind

	Use this command to display global IP address-MAC address binding.
	show address-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 global IPv4 address-MAC address binding.

```
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 Description	N/A

7.6 show address-bind uplink

	Use this command to display the exception port.
	show address-bind uplink

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 exception port. `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 not.

Related Commands	**Command**	**Description**
	address-bind uplink	Sets the exception port.
Platform Description	N/A	

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**
	days	Sets the password lifecycle, in the range from 1 to 65,535 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**
	length	Sets the minimum length of the password, in the range from 1 to 31.

Defaults	No minimum length of the password is set by default.
Command Mode	Global configuration 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 Examples	The following example sets the minimum length of the password to 8. `Ruijie(config)# password policy min-size 8`

Related Commands	**Command**	**Description**
	N/A	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**
	times	The past several times when passwords are configured, in the range from 1 to 31.

Defaults	This function is disabled by default.
Command	Global configuration mode

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 Examples	The following example bans the use of passwords used in the past five times. `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. Use the **no** form of this command to restore the default setting.
	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. The password the same as the username. 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 Examples	The following example configures the strong password check. `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 Examples	The following example encrypts the password: `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	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 Examples

The following example displays the password security policy set by the user.

```
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	N/A
Platform Description	N/A	

9 Port Security Commands

9.1 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.	
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

9.2 switchport port-security aging

	Use this command to set the aging time for all secure addresses on an interface. 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. Use the **no** form of this command to apply the aging time on automatically learned address or to disable the aging.	
	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 *time*	Specifies the aging time for the secure address on this port. Its range is 0-1440 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.	
Configuration Examples	The following example sets the aging time for all secure addresses on interface gigabitethernet 1/1 to eight minutes. `Ruijie(config)# interface gigabitethernet 1/1` `Ruijie(config-if)# switchport port-security aging time 8` `Ruijie(config-if)# switchport port-security aging static`	
Related Commands	**Command**	**Description**
	show port-security	Displays port security settings.
Platform	N/A	

Description	

9.3 switchport port-security binding

	Use this command 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 this command to remove the binding addresses.
	switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }
	no 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 { *ipv4-address* | *ipv6-address* }

Parameter Description	Parameter	Description
	mac-address	The source MAC addresses to be bound
	vlan_id	Vlan id of the binding source MAC address
	ipv4-address	Binding IPv4 addresses
	ipv6-address	Binding IPv6 addresses

Defaults	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A
Configuration Examples	The following example binds the IP address 192.168.1.100 on interface g 0/10: `Ruijie(config)#inter g0/10` `Ruijie(config-if)# switchport port-security binding 192.168.1.100` The following example shows how to bind the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with vlan id 1 on interface g 0/10 `Ruijie(config)#inter g0/10` `Ruijie(config-if)# switchport port-security binding 00d0.f800.5555 vlan 1 192.168.1.100`

Related Commands	Command	Description
	switchport 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 Description	N/A	

9.4 switchport port-security interface binding

	Use this command 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 this command to remove the binding addresses	
	switchport port-security interface i*nterface-id* **binding** [*mac-address* **vlan** *vlan_id*] {*ipv4-address*	*ipv6-address* }	
	no switchport port-security interface i*nterface-id* **binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address*	*ipv6-address* }	
	switchport port-security binding interface *interface-id* { *ipv4-address*	*ipv6-address* }	
	no switchport port-security binding interface *interface-id* { *ipv4-address*	*ipv6-address* }	
Parameter Description	**Parameter**	**Description**
	interface-id	Binding interface ID
	mac-address	Binding source MAC address
	vlan_id	Vlan ID of the binding source MAC address
	ipv4-address	Binding IPv4 address
	ipv6-address	Binding IPv6 address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example binds the IP address *192.168.1.100* on the interface *g 0/10*. `Ruijie(config)# switchport port-security binding interface g 0/10 192.168.1.100`	

	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(config)# switchport port-security binding interface g 0/10 00d0.f800.5555 vlan 1 192.168.1.100`

Related Commands	**Command**	**Description**
	switchport 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 Description	N/A

9.5 switchport port-security mac-address

	Use this command to configure manually the static secure address in the interface configuration mode. Use the **no** form of this command to remove the configuration.
	switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]
	no switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

Parameter Description	**Parameter**	**Description**
	mac-address	Static secure MAC address.
	vlan-id	Vlan ID of the MAC address. The configuration of vlan-id 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(config)#inter g0/10` `Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2`
Related Commands	**Command** / **Description**
	switchport 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 Description	N/A

9.6 switchport port-security interface mac-address

	Use this command to configure manually the static secure address in the privileged EXEC mode. 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**
	interface-id — Interface ID.
	mac-address — Static secure address
	vlan-id — VLAN ID of the MAC address. The configuration of vlan-id is only supported on the TRUNK port.
Defaults	N/A
Command Mode	Privileged EXEC 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(config)# switchport port-security interface g0/10 mac-address`

	`00d0.f800.5555 vlan 2`

Related Commands	Command	Description
	switchport 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 Description	N/A

9.7 switchport port-security maximum

	Use this command to set the maximum number of the port secure address. 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
	value	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(config)#inter g0/10` `Ruijie(config-if)# switchport port-security maximum 2`

Related Commands	Command	Description
	switchport 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 Description	N/A	

9.8 switchport port-security mac-address sticky

	Use this command to configure manually the Sticky MAC secure address in the interface configuration mode. 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. The **no** form of this command disables the Sticky MAC address learning.	
	switchport port-security mac-address sticky	
	no switchport port-security mac-address sticky	
Parameter Description	**Parameter**	**Description**
	mac-address	Static secure address.
	vlan-id	Vlan ID of the MAC address. The configuration of vlan-id is only supported on the TRUNK port.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the MAC address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 to 2 respectively: `Ruijie(config)#inter g0/10` `Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2` The following example enables the Sticky MAC address learning on interface g0/10: `Ruijie(config)#inter g0/10`	

	`Ruijie(config-if)# switchport port-security sticky mac-address`

Related Commands	Command	Description
	switchport 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 Description	N/A

9.9 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 *interface-id*	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	The following example displays the port security statistics: `Ruijie#show port-security`

Examples

```
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 address 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.
Secure Static 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 address bindings.
IPv6-ONLY Binding Addresses	The number of IPv6 address 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 Description	N/A

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**
	interface-type interface-number	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 gigabitethernet 1/1` `Interface Broadcast Control Multicast Control Unicast Control` `---------- --------------- --------------- ---------------` `Gi1/1 Disabled Disabled Disabled`	
Related Commands	**Command**	**Description**
	storm-control	Enables storm suppression.
Platform Description	N/A	

10.2 storm-control

	Use this command to enable the storm suppression for 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 *percent*	Sets the bandwidth percentage, for example, 20 means 20%
	pps *packets*	Sets the pps, which means packets per second
	rate-bps	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). Use the **show storm-control** command to display configuration.
Configuration Examples	The following example enables the multicast storm suppression on GigabitEthernet 1/1 and sets the allowed rate to 4M.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if)# storm-control multicast 4096
Ruijie(config-if)# end
```

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 Description	**Parameter**	**Description**
	rsa	Generates an RSA key.
	dsa	Generates a DSA key.
Defaults	By default, the SSH server does not generate a public key.	
Command Mode	Global configuration 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. ⚠ A key can be deleted by using the **crypto key zeroize** command. The **no crypto key generate** command is not available.	
Configuration Examples	The following example generates a RSA key to the SSH server: `Ruijie# configure terminal` `Ruijie(config)# 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 Description	N/A	

11.2 crypto key zeroize

	Use this command to delete a public key to the SSH server.

	crypto key zeroize { **rsa	dsa** }	
Parameter Description	**Parameter**	**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 Examples	The following example deletes a RSA key to the SSH server. `Ruijie# configure terminal` `Ruijie(config)# crypto key zeroize rsa`	
Related Commands	**Command**	**Description**
	show ip ssh	Displays the current status of the SSH server.
	crypto key generate { **rsa|dsa** }	Generates DSA and RSA keys.
Platform Description	N/A	

11.3 disconnect ssh

	Use this command to disconnect the established SSH connection.	
	disconnect ssh [**vty**] *session-id*	
Parameter Description	**Parameter**	**Description**
	vty	Established VTY connection.
	session-id	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 *line_number*	Disconnects the current VTY connection.

Platform Description	N/A

11.4 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 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 SCP functions. `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	

11.5 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 Description	**Parameter**	**Description**
	retry times	Authentication retry times, ranging from 0 to 5.
Defaults	The default is 3.	
Command Mode	Global configuration 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 Examples	The following example sets the authentication retry times to 2. `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 Description	N/A	

11.6 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 Description	**Parameter**	**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 Mode	Global configuration mode	
Usage Guide	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 Examples	The following example enable CTR encryption mode. `Ruijie# configure terminal` `Ruijie(con fig)# ip ssh cipher-mode ctr`	
Platform Description	N/A	

11.7 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 Description	**Parameter**	**Description**
	md5	MD5 algorithm
	md5-96	MD5-96 algorithm
	sha1	SHA1 algorithm
	sha1-96	SHA1-96 algorithm
Defaults	By default, SSHv2 supports all the algorithms.	
Command Mode	Global configuration mode	
Usage Guide	Ruijie SSHv1 servers do not support algorithms for message authentication.	
Configuration Examples	The following example sets the algorithm for message authentication to SHA1.	

	`Ruijie# configure terminal` `Ruijie(con fig)# ip ssh hmac-algorithm sha1`
Platform Description	N/A

11.8 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.	
	ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*	
	no ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*	
Parameter Description	**Parameter**	**Description**
	username	User name.
	filename	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 Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets RSA and DSA key files associated with user **test**. `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 Commands	**Command**	**Description**
	show ip ssh	Displays the current status of the SSH server.
Platform Description	N/A	

11.9 ip ssh time-out

	Use this command to set the authentication timeout interval 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**
	time	Authentication timeout interval, 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

11.10 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 Description	**Parameter**	**Description**
	1	Supports the SSH1 client connection request.
	2	Supports the SSH2 client connection request.

Defaults	SSH1 and SSH2 are compatible by default.
Command Mode	Global configuration 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 Examples	The following example sets the version of the SSH server. `Ruijie# configure terminal` `Ruijie(config)# ip ssh version 2`

Related Commands	**Command**	**Description**
	show ip ssh	Displays the current status of the SSH server.

Platform Description	N/A

11.11 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 Description	**Parameter**	**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# show crypto key mypubkey rsa`

Related Commands	**Command**	**Description**
	crypto key generate { **rsa** | **dsa** }	Generates DSA and RSA keys.

Platform Description	N/A

11.12 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 Mode	Privileged EXEC mode / Global configuration 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. Note: If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH version has been configured.	
Configuration Examples	The following example displays the information of the SSH server. `Ruijie# show ip ssh`	
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 Description	N/A	

11.13 show ssh

	Use this command to displays the information about the established SSH connection.	
	show ssh	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode / Global configuration 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 Examples	The following example displays the information about the established SSH connection: `Ruijie# show ssh`	
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 *interface-name*	Displays statistics on the specified interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	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**
	showip urpf	Displays the URPF configuration and statistics.
Platform Description	N/A	

ip verify unicast source reachable-via (Interface Configuration Mode)

	Use this command to enable the 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**]	
	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.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration 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. Not support the ACL association; Not support to use the IPv6 route with prefix in 65~127 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 Examples	The following example checks the URPF feature of the received packets in the strict mode on the interface GigabitEthernet 0/1. `Ruijie(config)# interface gigabitEthernet0/1` `Ruijie(config-if)# ip verify unicast source reachable-via rx`	
Related Commands	**Command**	**Description**

	show ip urpf	Displays the URPF information.
Platform Description	N/A	

12.2 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**
	seconds	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	N/A	
Configuration Examples	The following example set sthe URPF drop-rate compute interval as 60 seconds. `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 Description	N/A	

12.3 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 Mode	Interface configuration 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 Examples	The following example enables the URPF drop-rate monitoring on port GigabitEthernet 0/1. `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 Description	N/A

12.4 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**
	seconds / 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 1 minute. `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

12.5 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 *rate-value*	Sets the URPF drop-rate threshold, in the range from 0 to 4,294,967,295 in the unit of packets per second (pps).

Defaults	The default is 1000 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 Examples	The following example sets the URPF drop-rate threshold 10pps on the interface GigabitEthernet 0/1. `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 Description	N/A

12.6 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 *interface-name*	Displays the configuration and statistics on the specified interface.

Defaults	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Command Mode	Privileged EXEC mode
Usage Guide	The global configuration and statistics of all interfaces are displayed by default.
Configuration Examples	The following example displays IPv4 URPF configuration and statistics on port GigabitEthernet 0/1.

```
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**
	device_num	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.
	slot_num	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 Examples	The following example clears the CPP statistics:	

```
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        600      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
-----------------  -------------  --------------  ---------  ---------
```

	-------- ---------- bpdu 6 200 0 0 0 0
Related Commands	**Command** / **Description**
	N/A / N/A
Platform Description	N/A

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 Examples	The following example clears the CPP statistics on the supervisor module. Ruijie(config)#show cpu-protect type bpdu Packet Type Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) Total Total Drop ------------------ ------------- -------------- --------- --------- -------- ---------- bpdu 6 200 0 0 600 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 ------------------ ------------- -------------- --------- --------- -------- ---------- bpdu 6 200 0 0 0 0

Related Commands	**Command** / **Description**
	N/A / N/A
Platform Description	N/A

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**
	bandwidth_value / An integer number ranges from 0 to 100000 (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 32000 pps. `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 Description	N/A

13.4 cpu-protect traffic-class counters 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**
	traffic-class-num	An default integer that varies with products, indicating the queue priority.
	bandwidth_value	An integer number ranges from 0 to 100000 (pps). Indicates the bandwidth value of the CPU port.

Defaults	The default bandwitdth of each priority queue varies with products.
Command Mode	Global configuration mode
Usage Guide	N/A
Configuration Examples	The following example 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-protect 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**
	packet-type	Packet type, which varies with products.
	bandwidth_value	An integer number ranges from 0 to 100000 (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 BPDU bandwidth to 200 pps.

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect type bpdu bandwitdth 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 Description	N/A	

13.6 cpu-protect type packet-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**

	packet-type	Packet type, which varies with products.
	traffic-class-num	An integer number ranges from 0 to 100000 (PPS). Indicates the bandwidth value of the CPU port.
Defaults	The default PQ varies with products.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the PQ of BPDU packets to 5. `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` `------------------ ------------- -------------- --------- --------- -------- ----------` `bpdu 5 200 0 0 0 0`	

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

13.7 show cpu-protect

	Use this command to display all CPP configurations and statistics.	
	show cpu-protect [**device** *device_num*] [**slot** *slot_num***]**	
Parameter Description	**Parameter**	**Description**
	device_num	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.
	slot_num	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 modes	
Usage Guide	N/A	
Configuration Examples	The following example displays all CPP configurations and statistics of a line card:	

```
Ruijie#show cpu-protect slot 3/2

%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

------------------  -------------  --------------  ---------  ---------
--------  ----------

bpdu              6            128           0        0        0        0

arp               3           10000          0        0        0        0

arp-dai            3            10000          0        0        0        0

arp-proxy          3            10000          0        0        0        0

tpp               7           128           0        0        0        0

dot1x              4            128           0        0        0        0

gvrp               5            128           0        0        0        0

rldp               6            128           0        0        0        0
```

lacp	6	128	0	0	0	0
rerp	6	128	0	0	0	0
reup	6	128	0	0	0	0
lldp	5	128	0	0	0	0
cdp	5	128	0	0	0	0
dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
tunnel-bpdu	5	128	0	0	0	0
tunnel-gvrp	5	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0
stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0
dvmrp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0
rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0
vrrp6	6	128	0	0	0	0

	ttl0 6 128 0 0 0 0 ttl1 6 128 0 0 0 0 err_hop_limit 1 800 0 0 0 0 local-ipv4 6 128 0 0 0 0 local-ipv6 6 128 0 0 0 0 route-host-v4 0 4096 0 0 0 0 route-host-v6 0 4096 0 0 0 0 mld 0 1000 0 0 0 0 nd-snp-ns-na 6 128 0 0 0 0 nd-snp-rs 6 128 0 0 0 0 nd-snp-ra-redirect 6 128 0 0 0 0 nd-non-snp 6 128 0 0 0 0 erps 4 128 0 0 0 0 mpls-ttl0 6 128 0 0 0 0 mpls-ttl1 6 128 0 0 0 0 mpls-ctrl 6 128 0 0 0 0 isis 5 2000 0 0 0 0 bgp 1 128 0 0 0 0 cfm 0 128 0 0 0 0 fcoe-fip 6 128 0 0 0 0 fcoe-local 6 128 0 0 0 0 bfd-echo 6 5120 0 0 0 0 bfd-ctrl 6 5120 0 0 0 0 madp 7 1000 0 0 0 0 ip4-other 6 128 0 0 0 0 ip6-other 6 128 0 0 0 0 non-ip-other 6 20000 0 0 0 0 trill 2 1000 0 0 0 0 trill-oam 2 1000 0 0 0 0 efm 2 1000 0 0 0 0

Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

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	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	N/A
Platform Description	N/A	

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 configurations 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

------------------  -------------  --------------  ---------  ---------
--------  ----------

bpdu              6            128           0        0        0        0

arp               3           10000          0        0        0        0

arp-dai            3            10000          0        0        0        0

arp-proxy          3            10000          0        0        0        0

tpp               7           128           0        0        0        0

dot1x             4            128           0        0        0        0

gvrp              5            128           0        0        0        0

rldp              6            128           0        0        0        0

lacp              6            128           0        0        0        0

rerp              6            128           0        0        0        0

reup              6            128           0        0        0        0

lldp              5            128           0        0        0        0

cdp               5           128           0        0        0        0
```

dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
tunnel-bpdu	5	128	0	0	0	0
tunnel-gvrp	5	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0
stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0
dvmrp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0
rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0
vrrp6	6	128	0	0	0	0
ttl0	6	128	0	0	0	0
ttl1	6	128	0	0	0	0
err_hop_limit	1	800	0	0	0	0
local-ipv4	6	128	0	0	0	0
local-ipv6	6	128	0	0	0	0

	route-host-v4 0 4096 0 0 0 0 route-host-v6 0 4096 0 0 0 0 mld 0 1000 0 0 0 0 nd-snp-ns-na 6 128 0 0 0 0 nd-snp-rs 6 128 0 0 0 0 nd-snp-ra-redirect 6 128 0 0 0 0 nd-non-snp 6 128 0 0 0 0 erps 4 128 0 0 0 0 mpls-ttl0 6 128 0 0 0 0 mpls-ttl1 6 128 0 0 0 0 mpls-ctrl 6 128 0 0 0 0 isis 5 2000 0 0 0 0 bgp 1 128 0 0 0 0 cfm 0 128 0 0 0 0 fcoe-fip 6 128 0 0 0 0 fcoe-local 6 128 0 0 0 0 bfd-echo 6 5120 0 0 0 0 bfd-ctrl 6 5120 0 0 0 0 madp 7 1000 0 0 0 0 ip4-other 6 128 0 0 0 0 ip6-other 6 128 0 0 0 0 non-ip-other 6 20000 0 0 0 0 trill 2 1000 0 0 0 0 trill-oam 2 1000 0 0 0 0 efm 2 1000 0 0 0 0

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

13.10 show cpu-protect summary

	Use this command to display the CPP configurations 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	The following example displays the CPP configurations and statistics of the master device.	

```
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
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu               6              128             0          0          0          0
arp                3              10000           0          0          0          0
arp-dai             3              10000           0          0          0          0
arp-proxy           3              10000           0          0          0          0
```

tpp	7	128	0	0	0	0
dot1x	4	128	0	0	0	0
gvrp	5	128	0	0	0	0
rldp	6	128	0	0	0	0
lacp	6	128	0	0	0	0
rerp	6	128	0	0	0	0
reup	6	128	0	0	0	0
lldp	5	128	0	0	0	0
cdp	5	128	0	0	0	0
dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
tunnel-bpdu	5	128	0	0	0	0
tunnel-gvrp	5	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0
stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0
dvmrp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0

rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0
vrrp6	6	128	0	0	0	0
ttl0	6	128	0	0	0	0
ttl1	6	128	0	0	0	0
err_hop_limit	1	800	0	0	0	0
local-ipv4	6	128	0	0	0	0
local-ipv6	6	128	0	0	0	0
route-host-v4	0	4096	0	0	0	0
route-host-v6	0	4096	0	0	0	0
mld	0	1000	0	0	0	0
nd-snp-ns-na	6	128	0	0	0	0
nd-snp-rs	6	128	0	0	0	0
nd-snp-ra-redirect	6	128	0	0	0	0
nd-non-snp	6	128	0	0	0	0
erps	4	128	0	0	0	0
mpls-ttl0	6	128	0	0	0	0
mpls-ttl1	6	128	0	0	0	0
mpls-ctrl	6	128	0	0	0	0
isis	5	2000	0	0	0	0
bgp	1	128	0	0	0	0
cfm	0	128	0	0	0	0
fcoe-fip	6	128	0	0	0	0
fcoe-local	6	128	0	0	0	0
bfd-echo	6	5120	0	0	0	0
bfd-ctrl	6	5120	0	0	0	0
madp	7	1000	0	0	0	0
ip4-other	6	128	0	0	0	0
ip6-other	6	128	0	0	0	0
non-ip-other	6	20000	0	0	0	0
trill	2	1000	0	0	0	0
trill-oam	2	1000	0	0	0	0

	efm 2 1000 0 0 0 0
Related Commands	**Command** / **Description**
	N/A / N/A
Platform Description	N/A

13.11 show cpu-protect traffic-class

	Use this command to display the summarized configurations and statistics of priority queues.
	show cpu-protect traffic-class {*traffic-class-num* **| all} [device** *device_num***] [slot** *slot_num***]**

Parameter Description	**Parameter**	**Description**
	traffic-class-num	An default integer that varies with products, indicating the queue priority.
	all	Displays configurations and statistics of all priority queues.
	device_num	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.
	slot_num	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 configurations and statistics of priority queues.

```
R 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 Description	N/A	

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**
	packet-type	Packet type, which varies with products.
	device_num	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.
	slot_num	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 statistics of the ICMP packets. `Ruijie(config)#show cpu-protect type icmp` `Packet Type Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) Total Total Drop` `------------------ ------------- -------------- --------- --------- -------- ----------` `icmp 5 1500 50 0 10000 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**
	mac	Specifies the user MAC address to be cleared.
	vlan-id	Specifies the ID of the VLAN to be cleared.
	ip	Specifies the IP address to be cleared.
	interface-id	Specifies the ID of the interface to be cleared.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If users want to clear the current dynamic user information from the DHCP Snooping binding database, use this command.	
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. Note that DHCP Snooping cannot coexist with private VLAN.
Configuration Examples	The following example enables the DHCP Snooping function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping 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)
------------------------    -------    ---------------
```

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	N/A	

Description	

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 Boop 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
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)
-----------------------  -------    ------------
```

Related Commands	**Command**	**Description**
	show ip dhcp snooping	Displays the configuration of the DHCP Snooping.

Platform Description	N/A

14.4 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**
	time	The interval (600-86400) at which the system writes the dynamic user information of the DHCP Snooping database into the flash.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This function can avoid loss of user information after restart. In that case, users need to obtain IP addresses again for normal communication.	
Configuration Examples	The following example sets the interval at which the switch writes the user information into the flash to 3600 seconds: `Ruijie# configure terminal` `Ruijie(config)# ip dhcp snooping database write-delay 3600` `Ruijie(config)# end` `Ruijie# show ip dhcp snooping` `Switch DHCP snooping status: ENABLE` `DHCP snooping Verification of hwaddr field status: ENABLE` `DHCP snooping database write-delay time: 3600` `DHCP snooping option 82 status: DISABLE` `DHCP Snooping Support Bootp bind status: ENABLE` `Interface Trusted Rate limit (pps)` `------------------------ ------- ---------------`	
Related	**Command**	**Description**

Commands		
	show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.
Platform Description	N/A	

14.5 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 Examples	The following example writes the dynamic user information of the DHCP binding database into flash. `Ruijie# configure terminal` `Ruijie(config)# ip dhcp snooping database write-to-flash` `Ruijie(config)# end` `Ruijie#`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

14.6 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 message based on which the DHCP server assigns IP address.
Configuration Examples	The following example adds option82 to the DHCP request message.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                 :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time        :   0
DHCP snooping option 82 status                :   DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface              Trusted      Rate limit (pps)
------------------------ -------      ----------------
```


Related Commands	**Command**	**Description**
	show ip dhcp snooping	Displays the configuration of the DHCP Snooping.

Platform Description	N/A

14.7 ip dhcp snooping information option format remote-id

	Use this command to set the option82's 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 Description	**Parameter**	**Description**
	string *ascii-string*	The content of the option82's remote-id extension format is customized character string.
	hostname	The content of the option82's remote-id extension format hostname.

Defaults	This function is disabled by default.
Command Mode	Global configuration 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 being hostname: `Ruijie# configure terminal` `Ruijie(config)# ip dhcp snooping information option format remote-id hostname`

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

14.8 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 Mode	Interface configuration mode
Usage Guide	This command can deny all DHCP request messages under the port, that is, all the users under the port are prohibited to request addresses through DHCP.
Configuration Examples	The following example sets **fastethernet** 0/2 to be in the suppression status: `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 configuration information of the DHCP Snooping.
Platform Description	N/A	

14.9 ip dhcp snooping trust

	Use this command to set the ports of the switch as trusted ports. 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 untrust ports by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to set the port as trust port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrust port will be discarded.	

Configuration Examples	The following example sets **fastEthernet** *0/1* as a trust port: `Ruijie# configure terminal` `Ruijie(config)# interface fastEthernet 0/1` `Ruijie(config-if)# ip dhcp snooping trust` `Ruijie(config-if)# end` `Ruijie# show ip dhcp snooping` `Switch DHCP snooping status: ENABLE` `DHCP snooping 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)` `----------- ------- ----------` `FastEthernet0/1 yes unlimited`

Related Commands	**Command**	**Description**
	show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.
Platform Description	N/A	

14.10 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 enable checking the validity of the source MAC address of the DHCP request message. Once the function is enabled, the system will discard the DHCP request message that fails to pass the source MAC address check.
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` `Ruijie# show ip dhcp snooping` `Switch DHCP snooping status: ENABLE` `Verification of hwaddr field status: ENABLE` `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)`

Related Commands	**Command**	**Description**
	show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.
Platform Description	N/A	

14.11 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**
	vlan-rng	VLAN range of effective DHCP Snooping.
	vlan-min	Minimum VLAN of effective DHCP Snooping.
	vlan-max	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 configure effective DHCP Snooping VLAN by character string.
Configuration Examples	The following example enables the DHCP Snooping function in VLAN1000. `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	

14.12 ip dhcp snooping vlan information option change-vlan-to vlan

	Use this command to enable the option82's sub-option circuit 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**
	vlan-id	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 VLAN4094 in the option82's 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 Description	N/A

14.13 ip dhcp snooping vlan information option format-type circuit-id string

	Use this command to configure the option82's 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**
	vlan-id	The VLAN where the DHCP request packets are.
	ascii-string	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, 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 being *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 Description	This command is supported on all switches.

14.14 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
	vlan-word	The VLAN range.
	user-number	The maximum number of users bound with the VLAN.

Defaults	The limit for the number of users bound with the VLAN 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 Examples	The following example sets the maximum number of users bound with VLAN 1-10 and VLAN 20 to 30 respectively. 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 Description	N/A	

14.15 renew ip dhcp snooping database

	When the DHCP Snooping function is enabled, 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.	
Configuration Examples	The following example imports the flash file information to the DHCP Snooping database. `Ruijie# renew ip dhcp snooping database`	
Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	This command is supported on all switches.	

14.16 show ip dhcp snooping

	Use this command to display the setting of the DHCP Snooping.	
	show ip dhcp snooping	
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 information of DHCP Snooping. `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)` `------------------------ ------- ------------`

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 Description	N/A	

14.17 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	N/A	
Configuration Examples	The following example displays the information of the DHCP Snooping binding database. `Ruijie# show ip dhcp snooping binding` `Total number of bindings: 1` `MacAddress IpAddress Lease Type VLAN Interface` `00d0.f801.0101 192.168.1.1 - static 1 fastethernet 0/1`	
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 corresponding ARP filtering information according to the legal user information, implementing the illegal ARP packet filtering on the network.	
Configuration Examples	This 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` `Ruijie# configure terminal`	
Related Commands	**Command**	**Description**
	show interface arp-check list	Displays the ARP check entry information.
Platform Description	N/A	

15.2 show interface 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**
	interface-type — Wired interface type
	interface-number — Wired interface number
	Privileged EXEC mode
Usage Guide	Use this command to display the ARP check entries.
Configuration Examples	The following example displays the ARP check entries.

```
Ruijie(config)#show interface arp-check list
INTERFACE                    SENDER MAC      SENDER IP            POLICY SOUR
CE
----------------------- --------------- --------------- --------------------
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 a Layer2 port as trusted. Use the **no** form of this command to restore the default setting.	
	ip arp inspection trust	
	no ip arp inspection trust	
Parameter Description	**Parameter**	**Description**
	N/A	N/A
Defaults	The Layer2 port is an untrusted port by default.	
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 as trusted, 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 trusted. `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	On the NFPP-supported switches, interface rate is limited by NFPP rather than DAI. Therefore, if you execute this command on NFPP-supported switches, only the interface trust state will be displayed.	

16.2 ip arp inspection vlan

	Use this command to enable the DAI function for the VLAN. Use the **no** form of this command to

	disable DAI.
	ip arp inspection vlan { *vlan-id* | *word* }
	no ip arp inspection vlan { *vlan-id* | *word* }

Parameter Description	**Parameter**	**Description**
	vlan-id	VLAN ID. The range is from 1 to 4,094.
	word	VLAN range. For example, 1, 3-5, 7, 9-11.

Defaults	DAI is disabled by default.
Command Mode	Global configuration mode
Usage Guide	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 Examples	The following example enables the DAI function for VLAN 1. `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 Description	N/A	

16.3 show ip arp inspection vlan

	Use this command to display whether the DAI function is enabled for the VLAN.
	show ip arp inspection vlan [*vlan-id* | *word*]

Parameter Description	**Parameter**	**Description**
	vlan-id	VLAN ID. The range is from 1 to 4,094.
	word	VLAN range. for example, 1, 3-5, 7, 9-11.

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	The following example displays whether the DAI function is enabled for all VLANs. `Ruijie# show ip arp inspection vlan` `Vlan Configuration` `---- -------------` `1 Active`

Field	Description
Vlan	**VLAN number.**
Configuration	DAI status (active / inactive)

Related Commands	**Command**	**Description**
	N/A	N/A
Platform Description	N/A	

16.4 show ip arp inspection interface

	Use this command to display whether the DAI function is enabled for the interface.
	show ip arp inspection interface

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 DAI function is enabled for all interfaces.	

Examples

```
Ruijie#show ip arp inspection interface

Interface        Trust State

---------------------    -----------

GigabitEthernet 0/1     Untrusted

GigabitEthernet 0/2     Untrusted

GigabitEthernet 0/3     Untrusted

GigabitEthernet 0/4     Untrusted

Default                      Untrusted
```

Field	Description
Interface	Interface name.
Trust State	DAI trust state.

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 restore the default setting.	
	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**
	mac-address	Adds user MAC address statically.
	vlan-id	Adds user vlan id statically.
	ip-address	Adds user IP address statically.
	interface-id	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	N/A	
Configuration Examples	The following example configures a static user. `Ruijie# configure terminal` `Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface FastEthernet 0/1` `Ruijie(config)# end` `Ruijie# show ip source binding` `MacAddress IpAddress Lease(sec) Type VLAN Interface` `------------- --------- ---------- ---- ---- ------------` `0000.0000.0001 1.1.1.1 infinite static 1 FastEthernet 0/1` `Total number of bindings: 1`	
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. 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 configures IP Source Guard on port fastEthernet 0/1: `Ruijie# configure terminal` `Ruijie(config)# interface fastEthernet 0/1` `Ruijie(config-if)# ip verify source` `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**
	vlan-id	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	1. 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. 2. Once the IP source guard function is disabled, the excluded VLAN is cleared automatically. 3. This command is supported on the wired L2 switching port, AP port, and subinterface. 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 Description	N/A	

17.4 show ip source binding

	Use this command to display the binding information of IP source address and database.

	show ip binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter Description	**Parameter**	**Description**
	ip-address	Displays user binding information of corresponding IP.
	mac-address	Displays user binding information of corresponding MAC.
	dhcp-snooping	Displays binding information of dynamic user.
	static	Displays binding information of static user.
	vlan-id	Displays user binding information of corresponding VLAN.
	interface-id	Displays user binding information of corresponding interface.

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	`Ruijie# show ip source binding static` `MacAddress IpAddress Lease(sec) Type VLAN Interface` `------------- --------- ---------- ---- ---- ------------` `0000.0000.0001 1.0.0.1 infinite static 1 FastEthernet 0/1` `Total number of bindings: 1`

Related Commands	**Command**	**Description**
	ip source binding	Sets the binding static user.
Platform Description	N/A	

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**
	interface-id	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-no-snooping-vlan**: the interface isn’t within the range of DHCP Snooping VLAN and IP Source Guard is inactive. **inactive-trust-port**: the interface is the trusted port controlled by DHCP Snooping and IP Source Guard is inactive. **active**: the interface is the untrusted port controlled by DHCP Snooping and IP Source Guard is active.
Configuration Examples	The following example displays user filtering entry of IP Source Guard. `Ruijie # show ip verify source` `Interface Filter-type Filter-mode Ip-address Mac-address VLAN` `--------- ----------- ----------- ---------- -------------- ----` `FastEthernet 0/3 ip active 3.3.3.3 1` `FastEthernet 0/3 ip active deny-all` `FastEthernet 0/4 ip+mac active 4.4.4.4 0000.0000.0001 1` `FastEthernet 0/4 ip+mac active deny-all`

Related Commands	**Command**	**Description**
	ip verify source	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.
	pps	Sets the attack threshold, in the range from 1 to 19999 in unit of pps.
Defaults	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	N/A	

Description	

18.2 arp-guard enable

	Use this command to enable the anti-ARP guard function globally. 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 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 Description	N/A	

18.3 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
	seconds	Sets the isolate time. The value is 0, or in the range from 30 to 86400 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	N/A	
Configuration Examples	The following example sets the arp-guard isolate time globally to 180 seconds. `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 Description	N/A	

18.4 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 Examples	The following example enable packet forwarding through NFPP isolation. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# arp-guard isolate-forwarding enable`
Related Commands	**Command** / **Description** N/A / N/A
Platform Description	N/A

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** *number* / 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 ARP 20,000 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 Description	N/A

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**
	seconds / 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 Examples	The following example sets the arp guard monitor time to 180 seconds. `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 Description	N/A	

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.
	pps	Sets the rate limit, in the range of 1 to 19,999.
Defaults	See the *Configuration Guide*.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the arp guard rate limit. `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 remove the configuration.
	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 Examples	The following example sets the port based arp guard rate limit.. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# arp-guard ratelimit-forwarding enable`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

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**
	pkt-cnt	Sets the scan threshold, in the range from 1 to 19,999.

Defaults	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 Examples	The following example sets the global scan threshold to 20pps. `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 Description	N/A

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**
	vid	Sets the VLAN ID.
	interface-id	Sets the interface name and number.
	ip-address	Sets the IP address.
	mac-address	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 Examples	The following example clears the monitored host isolation. `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 Description	N/A

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 Examples	The following example clears ARP scanning table. `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 Description	N/A

18.12 clear nfpp define hosts

	Use this command to clear the monitored hosts. If the host is isolated, you need to disisolate it.
	clear nfpp define *name* **hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]

Parameter Description	**Parameter**	**Description**
	name	Defines guard name
	vid	VLAN ID
	interface-id	Interface name
	ip-address	IP address
	ipv6-address	IPv6 address

Defaults	N/A
Command Mode	Privileged EXEC mode.
Usage Guide	Use this command without the parameter to clear all monitored hosts of custom types.
Configuration Examples	The following example clears the monitored hosts. `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 monitored host isolation.
	clear nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description	**Parameter**	**Description**
	vid	Sets the VLAN ID.
	interface-id	Sets the interface name and number.
	mac-address	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 Examples	The following example clears the monitored host isolation. `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 Description	N/A

18.14 clear nfpp dhcpv6-guard hosts

	Use this command to clear the monitored host isolation.
	clear nfpp dhcpv6-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description	**Parameter**	**Description**
	vid	Sets the VLAN ID.
	interface-id	Sets the interface name and number.
	mac-address	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 Examples	The following example clears the monitored host isolation. `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 Description	N/A	

18.15 clear nfpp icmp-guard hosts

	Use this command to clear the monitored host isolation.	
	clear nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	
Parameter Description	**Parameter**	**Description**
	vid	Sets the VLAN ID.
	interface-id	Sets the interface name and number.
	ip-address	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 Examples	The following example clears the monitored host isolation. `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 Description	N/A	

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
	vid	Sets the VLAN ID.
	interface-id	Sets the interface name and number.
	ip-address	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 Examples	The following example clears the monitored host isolation. `Ruijie# clear nfpp ip-guard hosts vlan 1 interface g0/1`	
Related Commands	**Command**	**Description**
	ip-guard attack-threshold	Sets the global attack threshold.
	nfpp ip-guard policy	Sets the limit threshold and attack threshold.
	show nfpp ip-guard hosts	Displays the monitored host.
Platform Description	N/A	

18.17 clear nfpp nd-guard hosts

	Use this command to remove the speed limit on the host. **clear nfpp nd-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]

Parameter Description	Parameter	Description
	vid	Sets the VLAN ID.
	interface-id	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`
Platform Description	N/A

18.18 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 Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears the NFPP log buffer area. `Ruijie# clear nfpp log`	
Related Commands	**Command**	**Description**
	show nfpp log	Displays the NFPP log configuration or the log buffer area.
Platform Description	N/A	

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_vaule*

	no cpu-protect sub-interface {*manage*|*protocol*|*route*} **percent**	
	default cpu-protect sub-interface {*manage*|*protocol*|*route*} **percent**	
Parameter Description	**Parameter**	**Description**
	percent_value	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: 20; 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	Configures the traffic bandwidth of each type of packets.
Platform Description	N/A	

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_vaule*	
	no cpu-protect sub-interface { *manage*	*protocol*	*route* } **pps**	
	default cpu-protect sub-interface { *manage*	*protocol*	*route* } **pps**	
Parameter Description	**Parameter**	**Description**
	pps_value	The rate limit threshold, in the range from 1 to 100,000
Defaults	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 2000 pps. `Ruijie(config)# cpu-protect sub-interface manage pps 2000`

Related Commands	**Command**	**Description**
	cpu-protect sub-interface { **manage** | **protocol** | **route** } **percent**	Configures the percent value of each type of packets occupied in the buffer area.

Platform Description	N/A

18.21 define

	Use this command to create the user-defined 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**
	name	Name of the user-defined anti-attack type.

Defaults	N/A
Command Mode	NFPP configuration mode
Usage Guide	Use this command to create a new user-defined anti-attack type.
Configuration Examples	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 user-defined anti-attack configuration
Platform Description	N/A	

18.22 define 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**
	name	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 Examples	The following example enabled the user-defined anti-attack globally. `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 Description	N/A	

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.
	pps	Sets the attack threshold, in pps. The valid range is 1 to 19999.

Defaults	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)# dhcp-guard attack-threshold per-src-mac 15` `Ruijie(config-nfpp)# dhcp-guard attack-threshold per-port 200`

Related Commands	**Command**	**Description**
	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 Description	N/A

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 Description	N/A

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**
	seconds / Sets the isolate time. The value is 0 or in the range from 30 to 86400 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**
	number	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 DHCP 20,000 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)# dhcp-guard monitored-host-limit 200`
Related Commands	**Command** / **Description** **show nfpp dhcp-guard summary** / Displays the configuration.
Platform Description	N/A

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** *seconds* / Sets the monitor time, in the range from 180 to 86,400 in the unit of 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 Examples	The following example sets the monitor time to 180 seconds. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# dhcp-guard monitor-period 180`
Related	**Command** / **Description**

Commands		
	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 Description	N/A	

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.
	pps	Sets the rate limit, in the range of 1 to 19,999.
Defaults	See the *Configuration Guide*.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the rate-limit threshold globally. `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 Description	N/A	

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.
	pps	Sets the attack threshold, in the range is from 1 to 19999 pps.
Defaults	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 Description	N/A	

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 Mode	NFPP configuration mode
Usage Guide	N/A
Configuration Examples	The following example enables the DHCPv6 anti-attack function globally. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# dhcpv6-guard enable`

Related Commands	**Command**	**Description**
	N/A	N/A

Platform Description	N/A

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**
	number	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 DHCPv6 20,000. 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)# dhcpv6-guard monitored-host-limit 200`

Related Commands	**Command**	**Description**
	show nfpp dhcpv6-guard summary	Displays the configuration.
Platform Description	N/A	

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**
	seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of 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 Examples	The following example sets the monitor time to 180 seconds. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# dhcpv6-guard monitor-period 180`

Related Commands	**Command**	**Description**
	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 isolated host.

Platform Description	N/A

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**
	per-src-mac	Sets the rate limit for each source MAC address.
	per-port	Sets the rate limit for each port.
	pps	Sets the rate limit, in the range from 1 to 19,999.

Defaults	See the *Configuration Guide*.
Command Mode	NFPP configuration mode
Usage Guide	N/A
Configuration Examples	The following example sets the rate-limit threshold globally. `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 Description	N/A

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.
	rate-limit-pps	Sets the rate-limit threshold.
	attack-threshold-pps	Sets the attack threshold.

Defaults	N/A
Command Mode	NFPP define configuration 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 *name* **policy**	Sets the rate-limit threshold and attack threshold.
	show nfpp define summary	Displays the user-defined anti-attack configuration
Platform Description	N/A	

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.
	pps	Sets the attack threshold, in the range from 1 to 19999 in the unit of pps.
Defaults	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)# 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 Description	N/A

18.36 icmp-guard enable

	Use this command to enable the ICMP anti-attack function. Use the **no** form of this command to disable the function. Use the **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 Mode	NFPP configuration mode
Usage Guide	N/A
Configuration Examples	The following example enables the ICMP anti-attack function globally. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# icmp-guard enable`

Related Commands	Command	Description
	nffp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
	show nfpp icmp-guard summary	Displays the configuration.

Platform Description	N/A

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**
	seconds	Sets the isolate time. The value is in the range is 0 or from 30 to 86400 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)# 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 Description	N/A	

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**
	number	The maximum monitored host number, in the range from 1 to 4294967295.
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 ICMP 20,000 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)# icmp-guard monitored-host-limit 200`	
Related Commands	**Command**	**Description**
	show nfpp icmp-guard summary	Displays the configuration.
Platform Description	N/A	

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	**Parameter**	**Description**

Description		
	seconds	Sets the monitor time, in the range from180 to 86400 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 Examples	The following example sets the monitor time to 180 seconds. `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 Description	N/A	

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.
	pps	Sets the rate limit, in the range from1 to19999.

Defaults	See the *Configuration Mode*.
Command Mode	NFPP configuration mode.
Usage Guide	N/A
Configuration Examples	The following example sets the rate-limit threshold globally. `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 Description	N/A

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**
	ip	Sets the IP address.
	mask	Sets the IP mask.
	all	Deletes the configuration of all trusted hosts.

Defaults	No trusted host is configured by default.
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 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 Examples	The following example sets the trusted hosts free form monitoring. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0`
Related Commands	**Command** / **Description**
	show nfpp icmp-guard trusted-host / Displays the configuration.
Platform Description	N/A

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 / Sets the attack threshold for each source IP address.
	per-port / Sets the attack threshold for each port.
	pps / Sets the attack threshold, in pps. The valid range is 1 to 19999.
Defaults	By default, the attack threshold for each source IP address and each port are 200pps and 400pps respectively.
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	Displays the rate-limit threshold and attack threshold.
	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 Description	N/A	

18.43 ip-guard enable

	Use this command to enable the IP anti-scan function. 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 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 IP anti-scan function globally. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# ip-guard enable`	
Related Commands	**Command**	**Description**
	nffp ip-guard enable	Enables the IP anti-scan function on the interface.
Platform Description	N/A	

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 Description	**Parameter**	**Description**
	seconds	Sets the isolate time. The value is 0 or in the range from 30 to 86400 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	N/A	
Configuration Examples	The following example sets the isolate time globally to 180 seconds. `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 Description	N/A	

18.45 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	**Parameter**	**Description**

Description		
	seconds	Sets the monitor time, in the range from 180 to 86400 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 Examples	The following example sets the monitor time to 180 seconds. `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 Description	N/A	

18.46 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**
	number	The maximum monitored host number, in the range from 1 to 4294967295.

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 IP 20,000 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)# ip-guard monitored-host-limit 200`

Related Commands	**Command**	**Description**
	show nfpp ip-guard summary	Displays the configuration.
Platform Description	N/A	

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.
	pps	Sets the rate limit, in the range of 1 to 19999.

Defaults	See the *Configuration Guide*.
Command Mode	NFPP configuration mode.

Usage Guide	N/A
Configuration Examples	The following example sets the rate-limit threshold globally. `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 Description	N/A

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**
	pkt-cnt	Sets the scan threshold, in the range from 1 to 19999.

Defaults	See the *Configuration Guide*.
Command Mode	NFPP configuration mode.
Usage Guide	N/A
Configuration Examples	The following example sets the global scan threshold to 20pps. `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 Description	N/A	

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**
	ip	Sets the IP address.
	mask	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 Examples	The following example sets the trusted hosts free form monitoring. `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** form of this command to store logs in the cache, instead of being displayed 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 Examples	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 Description	N/A

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**
	number	The buffer area size, in the range from 0 to 1024.

Defaults	The default is 256.
Command Mode	NFPP configuration mode.
Usage Guide	N/A
Configuration Examples	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 *number_of_message* **interval** *length_in_seconds*	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 Description	N/A	

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**
	number_of_message	The valid range is from 0 to1024. 0 indicates that all logs are recorded in the specific buffer area and no syslogs are generated.
	length_in_seconds	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 *number_of_message* and *length_in_seconds* values are 0, it indicates not to write the log to the buffer area but generate the syslog immediately. The parameter *number_of_message /length_in_second* 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 Mode	NFPP configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the rate of syslog generated from the NFPP log buffer area. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# log-buffer logs 2 interval 12`	
Related Commands	**Command**	**Description**
	log-buffer entries *number*	Sets the NFPP log buffer area size.
	show nfpp log summary	Displays the NFPP log configuration or the log buffer area.
Platform Description	N/A	

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**
	vlan-range	Sets the specified VLAN range, in the format such as “1-3, 5”.
	interface-id	Sets the interface ID.
Defaults	All logs are recorded by default.	
Command Mode	NFPP configuration mode.	

Usage Guide	Use this command to filter the logs and records the logs within the specified VLAN range or the specified port
Configuration Examples	The following example records the logs in VLAN 1,VLAN 2,VLAN 3 and VLAN 5 only. `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 Description	N/A	

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**
	type	Ethernet link layer packet type
	smac	Source MAC address
	smac_mask	Source MAC address mask
	dmac	Destination MAC address
	dmac_mask	Destination MAC address mask
	protocol	IPv4/v6 message protocol
	sip	Source IPv4 address
	sip_mask	Source IPv4 address mask
	sipv6	Source IPv6 address
	sipv6_masklen	Source IPv6 address mask
	dip	Destination IPv4 address
	dip_mask	Destination IPv4 address mask

	dipv6	Destination IPv6 address
	dipv6_masklen	Length of the destination IPv6 address mask.
	sport	Source port
	dport	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**
	number	The maximum monitored host number, in the range from 1 to 4294967295.
Defaults	The default is 20,000.	
Command	NFPP define 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_DEFINE_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of name's 20,000 monitored hosts. to remind the administrator
Configuration Examples	The following example sets the maximum monitored host number. `Ruijie(config)#nfpp` `Ruijie(config-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**
	seconds	Sets the monitor time, in the range from180 to 86400 in the unit of seconds.
Defaults	The default is 600.	
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 1000 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 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.
	pps	Sets the attack threshold, in the range from1 to 19999 in the unit of seconds.

Defaults	By default, the default attack threshold for the ns-na, rs and ra-redirect on each port is 5000, 1000 and 1000 respectively.
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)# 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 Description	N/A

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 Mode	NFPP configuration mode.
Usage Guide	N/A
Configuration Examples	The following example enables the ND anti-attack function. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# nd-guard enable`

Related	**Command**	**Description**

Commands		
	nffp nd-guard enable	Enables the ND anti-attack function on the interface.
	show nfpp nd-guard summary	Displays the configuration.
Platform Description	N/A	

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.
	pps	Sets the attack threshold, in the range is from 1 to 19999 in the unit of pps.
Defaults	See the *Configuration Guide*.	
Command Mode	NFPP configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the rate-limit threshold globally. `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 Description	N/A

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 Examples	The following example enables the ND-guard ratelimit-forwarding on the interface. `Ruijie(config)# nfpp` `Ruijie(config-nfpp)# nd-guard ratelimit-forwarding enable`	
Platform Description	N/A	

18.61 nfpp

	Use this command to enable 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 the NFPP configuration mode to configure further functions.
Configuration Examples	`Ruijie(config)# nfpp`
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. `Ruijie(config)# interface G0/1` `Ruijie(config-if)# nfpp arp-guard enable`	
Related Commands	**Command**	**Description**
	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**
	seconds	Sets the isolate period. The value is 0, or in the range from 30 to 86400 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 Examples	The following example sets the isolate period in the interface configuration mode. `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 Description	N/A	

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.
	rate-limit-pps	Sets the rate-limit threshold , in the range from 1 to 19999.
	attack-threshold-pps	Sets the attack threshold, in the range from1 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**
	pkt-cnt	Sets the scan threshold, in the range from1 to 19999.

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 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 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**
	name	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 Examples	The following example enables the user-defined anti-attack function on the interface. `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 Description	N/A

18.67 nfpp define 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.
	rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19999.
	attack-threshold-pps	Sets the attack threshold, in the range of from1 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 local rate-limit threshold and the attack threshold.

	`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 Description	N/A

18.68 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 configuratio
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 Description	N/A

18.69 nfpp dhcp-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 dhcp-guard isolate-period { *seconds* | **permanent** }	
	no nfpp dhcp-guard isolate-period	
	default nfpp dhcp-guard isolate-period	
Parameter Description	**Parameter**	**Description**
	seconds	Sets the isolate period. The value is 0 or in the range from 30 to 86400 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 Examples	The following example sets the isolate period to 180 seconds. `Ruijie(config)# interface G0/1` `Ruijie(config-if)# nfpp dhcp-guard isolate-period 180`	
Related Commands	**Command**	**Description**
	dhcp-guard isolate-period	Sets the global isolate period.
	show nfpp dhcp-guard summary	Displays the configuration.
Platform Description	N/A	

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.
	rate-limit-pps	Sets the rate-limit threshold, in the range from1 to 19999.
	attack-threshold-pps	Sets the attack threshold, in the range from1 to 19999.
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 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 on interface G0/1. `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 Description	N/A	

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 Mode	Interface configuration mode	
Usage Guide	The interface DHCPv6 anti- attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the DHCPv6 anti-attack function on interface G0/1. `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 Description	N/A	

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.
	rate-limit-pps	Sets the rate-limit threshold, in the range of from1 to 19999.
	attack-threshold-pps	Sets the attack threshold, in the range from1 to19999.
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 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 Description	N/A	

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 Description	**Parameter**	**Description**
	N/A	N/A
Defaults	The ICMP anti-attack function is not enabled on the interface.	
Command Mode	Interface configuration mode.	
Usage Guide	The interface ICMP anti- attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the ICMP anti-attack function on the interface. `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 Description	N/A	

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**
	seconds	Sets the isolate period. The value is 0 or in the range from 30 to 86400 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 Examples	The following example sets the isolate period in the interface configuration mode. `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 *{ p***er-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.
	rate-limit-pps	Sets the rate-limit threshold, in the range from1 to 19999.
	attack-threshold-pps	Sets the attack threshold, in range from1 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 icmp-guard policy per-src-ip 5 10` `Ruijie(config-if)# nfpp icmp-guard policy per-port 100 200`	
Related Commands	**Command**	**Description**
	icmp-guard attack-threshold	Sets the global attack threshold.
	icmp-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp icmp-guard summary	Displays the configuration.
	show nfpp icmp-guard hosts	Displays the monitored host.
	clear nfpp icmp-guard hosts	Clears the isolated host.
Platform Description	N/A	

18.76 nfpp ip-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 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-scan function is not enabled on the interface.
Command Mode	Interface configuration mode
Usage Guide	The interface IP anti-scan configuration is prior to the global configuration.
Configuration Examples	The following example enables the ICMP anti-attack function on the interface. `Ruijie(config)# interface G0/1` `Ruijie(config-if)# nfpp ip-guard enable`

Related Commands	**Command**	**Description**
	ip-guard enable	Enables the anti-ARP attack function.
	show nfpp ip-guard summary	Displays the configuration.

Platform Description	N/A

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**
	seconds	Sets the isolate period, in the range from 30 to 86400 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 Examples	The following example sets the isolate period in the interface configuration mode. `Ruijie(config)# interface G0/1` `Ruijie(config-if)# nfpp ip-guard isolate-period 180`	
Related Commands	**Command**	**Description**
	ip-guard isolate-period	Sets the global isolate period.
	show nfpp ip-guard summary	Displays the configuration.
Platform Description	N/A	

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.
	rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19999.
	attack-threshold-pps	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 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 Description	N/A

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**
	pkt-cnt	Sets the scan threshold, in the range from 1 to 19999.

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 Description	N/A	

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 not enabled on the interface.	
Command Mode	Interface configuration mode.	
Usage Guide	The interface ND anti-attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the ND anti-attack function on the interface. `Ruijie(config)# interface G0/1` `Ruijie(config-if)# nfpp nd-guard enable`	
Related Commands	**Command**	**Description**
	nd-guard enable	Enables the ND anti- attack function.
	show nfpp nd-guard summary	Displays the configuration.
Platform Description	N/A	

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**
	ns-na	Sets the neighbor request and neighbor advertisement.
	rs	Sets the router request.
	ra-redirect	Sets the router advertisement and the redirect packets.
	rate-limit-pps	Sets the rate-limit 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 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**
	nd-guard attack-threshold	Sets the global attack threshold.
	nd-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp nd-guard summary	Displays the configuration.

Platform Description	N/A

18.82 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**
	statistics	Displays the statistical information of the monitored host.
	vid	The VLAN ID.
	interface-id	The interface name.
	ip-address	The IP address.
	mac-address	The MAC address.

Defaults	N/A
Command Mode	Privileged EXEC mode.
Usage Guide	N/A
Configuration Examples	The following example displays the statistical information of the monitored host.

```
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**
	clear nfpp arp-guard hosts	Clears the monitored host.

Platform Description	N/A

18.83 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**
	statistics	Displays the statistical information of the ARP scan list.
	vid	The VLAN ID.
	interface-id	The interface name.
	ip-address	The IP address.
	mac-address	The MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the ARP scan list.	

```
Ruijie# show nfpp arp-guard scan statistics

arp-guard scan table has 4 record(s).


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)


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
	arp-guard scan-threshold	Sets the global scan threshold.
	nfpp arp-guard scan-threshold	Sets the scan threshold.
	clear nfpp arp-guard scan	Clears the ARP scan list.

Platform Description	N/A

18.84 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 Examples	The following example displays the configuration. ``` 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. - / No configuration.

Related Commands	**Command**	**Description**
	arp-guard attack-threshold	Sets the global attack threshold.
	arp-guard enable	Enables the anti-ARP attack function.
	arp-guard isolate-period	Sets the global isolate time.
	arp-guard monitor-period	Sets the monitor period.
	arp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
	arp-guard rate-limit	Sets the global rate-limit threshold.
	arp-guard scan-threshold	Sets the global scan threshold.
	nfpp arp-guard enable	Enables the anti-ARP attack function on the interface.
	nfpp arp-guard isolate-period	Sets the isolate time.
	nfpp arp-guard policy	Sets the rate-limit threshold and attack threshold.
	nfpp arp-guard scan-threshold	Sets the scan threshold.
Platform Description	N/A	

18.85 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*]]]

Parameter Description	**Parameter**	**Description**
	name	Name of the user-defined anti-attack type.
	statistics	Displays the statistics of monitored hosts.
	vid	Vlan ID.

	interface-id	Interface name.
	ip-address	IP address.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command allows filtering the hosts with parameters specified	
Configuration Examples	The command execution as shown below means that there are 120 hosts monitored totally, wherein 100 hosts are isolated successfully, and 20 hosts fails. 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**
	clear nfpp define hosts	Clears the monitored hosts of user-defined anti-attack type.
Platform Description	N/A	

18.86 show nfpp define summary

	Use this command to display the configuration.	
	show nfpp define summary [*name*]	
Parameter Description	**Parameter**	**Description**
	name	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 Examples	The following example displays the configuration. `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.

Related Commands	**Command**	**Description**
	match	Clears the monitored hosts of user-defined anti-attack type.
	policy	Attack threshold and rate-limit threshold.
	isolate-period	Isolates time
	monitored-period	Monitored time
	monitored-host-limit	Maximum monitored host number
Platform Description	N/A	

18.87 show nfpp define trusted-host

	Use this command to display the trusted host free from monitoring.	
	show nfpp define trusted-host *name*	
Parameter	**Parameter**	**Description**

Description		
	name	Name of the user-defined anti-attack type.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the trusted host configuration. `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**
	trusted-host	Configures the trusted hosts.
Platform Description	N/A	

18.88 show nfpp dhcp-guard hosts

	Use this command to display the monitored host.	
	show nfpp dhcp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]	
Parameter Description	**Parameter**	**Description**
	statistics	Displays the statistical information of the monitored host.
	vid	The VLAN ID.
	interface-id	The interface name.
	ip-address	The IP address.
	mac-address	The MAC address.
Defaults	N/A	

Command Mode	Privileged EXEC mode.
Usage Guide	N/A
Configuration Examples	The following example displays the statistical information of the monitored host. `Ruijie# show nfpp dhcp-guard hosts statistics` `success fail total` `------- ---- -----` `100 20 120` `The following example shows 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**
	clear nfpp dhcp-guard hosts	Clears the monitored host.
Platform Description	N/A	

18.89 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 Examples	The following example displays the configuration.

```
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.
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.
-	No configuration.

Related Commands	**Command**	**Description**
	dhcp-guard attack-threshold	Sets the global attack threshold.
	dhcp-guard enable	Enables the DHCP anti-attack function.
	dhcp-guard isolate-period	Sets the global isolate time.
	dhcp-guard monitor-period	Sets the monitor period.
	dhcp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
	dhcp-guard rate-limit	Sets the global rate-limit threshold.
	nfpp dhcp-guard enable	Enables the DHCP anti-attack function on the interface.
	nfpp dhcp-guard isolate-period	Sets the isolate time.
	nfpp dhcp-guard policy	Sets the rate-limit threshold and attack

		threshold.
Platform Description	N/A	

18.90 show nfpp dhcpv6-guard hosts

	Use this command to display the monitored host.	
	show nfpp dhcpv6-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]	
Parameter Description	**Parameter**	**Description**
	statistics	Displays the statistical information of the monitored host.
	vid	The VLAN ID.
	interface-id	The interface name.
	ip-address	The IP address.
	mac-address	The MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example shows the monitored host: `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**
	clear nfpp dhcpv6-guard hosts	Clears the monitored host.
Platform Description	N/A	

18.91 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 Mode	Privileged EXEC mode.
Usage Guide	N/A
Configuration Examples	The following example displays the configuration.

```
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
```

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.
-	No configuration.

Related Commands	**Command**	**Description**
	dhcpv6-guard attack-threshold	Sets the global attack threshold.
	dhcpv6-guard enable	Enables the DHCPv6 anti-attack function.

	dhcpv6-guard monitor-period	Sets the monitor period.
	dhcpv6-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
	dhcpv6-guard rate-limit	Sets the global rate-limit threshold.
	nfpp dhcpv6-guard enable	Enables the DHCPv6 anti-attack function on the interface.
	nfpp dhcpv6-guard policy	Sets the rate-limit threshold and attack threshold.
Platform Description	N/A	

18.92 show nfpp icmp-guard hosts

	Use this command to display the monitored host.	
	show nfpp icmp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]	
Parameter Description	**Parameter**	**Description**
	statistics	Displays the statistical information of the monitored host.
	vid	The VLAN ID.
	interface-id	The interface name.
	ip-address	The IP address.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the statistical information of the monitored host. `Ruijie# show nfpp icmp-guard hosts statistics` `success fail total` `------- ---- -----` `100 20 120` The following example displays the monitored host. `Ruijie# show nfpp icmp-guard hosts` `If column 1 shows '*', it means "hardware failed to isolate host".`	

	VLAN interface IP address remain-time(s) ---- -------- --------- ------------- 1 Gi0/1 1.1.1.1 110 2 Gi0/2 1.1.2.1 61 Total:2 host(s)

Related Commands	Command	Description
	clear nfpp icmp-guard hosts	Clears the monitored host.
Platform Description	N/A	

18.93 show nfpp icmp-guard summary

	Use this command to display the configuration.
	show nfpp icmp-guard summary

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 configuration. Ruijie# show nfpp icmp-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 4/-/60 8/-/100 Gi 0/1 Enable 180 5/-/- 8/-/- Gi 0/2 Disable 200 4/-/60 8/-/100 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. -: No configuration.

Related Commands	Command	Description
	icmp-guard attack-threshold	Sets the global attack threshold.
	icmp-guard enable	Enables the ICMP anti-attack function.
	icmp-guard isolate-period	Sets the global isolate time.
	icmp-guard monitor-period	Sets the monitor period.
	icmp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
	icmp-guard rate-limit	Sets the global rate-limit threshold.
	nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
	nfpp icmp-guard isolate-period	Sets the isolate time.
	nfpp icmp-guard policy	Sets the rate-limit threshold and attack threshold.
Platform Description	N/A	

18.94 show nfpp icmp-guard trusted-host

	Use this command to display the trusted host free from being monitored.
	show nfpp icmp-guard summary

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 trusted host free from being monitored. `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**
	icmp-guard trusted-host	Sets the trusted host.
Platform Description	N/A	

18.95 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**
	statistics	Displays the statistical information of the monitored host.
	vid	The VLAN ID.
	interface-id	The interface name.
	ip-address	The IP address.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the statistical information of the monitored host. `Ruijie# show nfpp ip-guard hosts statistics`	

	success fail total ------- ---- ----- 100 20 120 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
	clear nfpp ip-guard hosts	Clears the monitored host.
Platform Description	N/A	

18.96 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 Examples	The following example displays the configuration. `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.
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.
-	No configuration.

Related Commands	Command	Description
	ip-guard attack-threshold	Sets the global attack threshold.
	ip-guard enable	Enables the IP anti-scan function.
	ip-guard isolate-period	Sets the global isolate time.
	ip-guard monitor-period	Sets the monitor period.
	ip-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
	ip-guard rate-limit	Sets the global rate-limit threshold.
	nfpp ip-guard enable	Enables the IP anti-scan function on the interface.
	nfpp ip-guard isolate-period	Sets the isolate time.
	nfpp ip-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description	N/A

18.97 show nfpp ip-guard trusted-host

	Use this command to display the trusted host free from being monitored.
	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 Examples	The following example displays the trusted host free from being monitored.

```
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**
	ip-guard trusted-host	Sets the trusted host.
Platform Description	N/A	

18.98 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**
	statistics / Displays the statistical information of the NFPP log buffer area.
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 Examples	The following example displays the NFPP log configuration. `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 16:23:10` `ARP 1 Gi0/1 1.1.1.1 - ISOLATED 2009-05-30 16:23:10` `ARP 1 Gi0/1 1.1.1.2 - DoS 2009-05-30 16:23:15` `ARP 1 Gi0/1 1.1.1.2 - ISOLATE_FAILED 2009-05-30 16:23:15` `ARP 1 Gi0/1 - 0000.0000.0001 SCAN 2009-05-30 16:30:10` `ARP - Gi0/2 - - PORT_ATTACKED 2009-05-30 16:30:10`

	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Protocol</td><td>ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT</td></tr><tr><td>Reason</td><td>1. DoS 2. ISOLATED 3. ISOLATE_FAILE 4. SCAN 5. PORT_ATTACKED</td></tr></table>
Related Commands	**Command** / **Description**
	clear nfpp log / Clears the NFPP log buffer area.
Platform Description	N/A

18.99 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 Examples	The following example displays the configuration. `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.
-	No configuration.

Related Commands	**Command**	**Description**
	nd-guard attack-threshold	Sets the global attack threshold.
	nd-guard enable	Enables the ND anti-attack function.
	nd-guard rate-limit	Sets the global rate-limit threshold.
	nfpp nd-guard enable	Enables the ND anti-attack function on the interface.
	nfpp nd-guard policy	Sets the rate-limit threshold and attack threshold.
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**
	statistics	Displays the statistics of the monitored host.
	vid	Sets the VLAN ID.
	interface-id	Sets the interface name and number.
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the statistics of the host monitored by ND-guard. `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 ```
Prompt Messages	N/A
Platform Description	N/A

18.101 trusted-host

	Use this command to set the trusted hosts free form monitoring. Use the no form of this command to restore the default setting.	
	trusted-host { *mac mac_mask* | *ip mask* | *IPv6/prefixlen* }	
	no trusted-host { **all** | *ip mask* | *IPv6/prefixlen* }	
Parameter Description	**Parameter**	**Description**
	ip	Sets the IP address.
	mac	MAC address.
	mac_mask	MAC address mask.
	IPv6/prefixlen	IPv6 address and mask length
	mask	IP mask.
	all	Deletes the configuration of all trusted hosts with the no form of this command.
Defaults	No trusted host is configured by default.	
Command	NFPP define 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. 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 Examples	The following example sets the trusted hosts free form monitoring. `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**
	show nfpp define trusted-host	Displays the trusted host configuration.
Platform Description	N/A	

18.102 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 Description	N/A
Command Mode	NFPP configuration 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 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 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 anti-attack of the self-consumption: `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**
	show ip deny invalid-l4port	Displays the state of anti-attack of the self-consumption.
Platform Description	N/A	

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 Description	**Parameter** / **Description**
	N/A / N/A
Defaults	The function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A
Configuration Examples	The following example enables the anti-attack of the invalid TCP packets: `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`
Related Commands	**Command** / **Description**
	show ip deny invalid-tcp / Displays the state of anti-attack of the invalid TCP packets.
Platform Description	N/A

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
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 anti-land-attack: `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 Description	N/A

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
Command Mode	Privileged
Usage Guide	N/A
Configuration Examples	The following example displays the state of the anti-DOS-attack. `Ruijie#show ip deny` `  Protect against Land attack            On` `  Protect against invalid L4port attack    Off` `  Protect against invalid TCP attack      Off`
Prompt Messages	N/A
Platform Description	N/A

19.5 show ip deny invalid-l4port

	Use this command to display the state of the anti-consumption-attack.
	show ip deny invalid-l4port
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 state of the anti-consumption-attack.

```
Ruijie# show ip deny invalid-l4port
 DoS Protection Mode                    State
--------------------------------       -----
 protect against invalid l4port attack  Off
```

Related Commands	**Command** / **Description**
	N/A / N/A
Platform Description	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
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 state of the anti-attack of the invalid TCP packets. `Ruijie# show ip deny invalid-tcp` `DoS Protection Mode State` `------------------------------------ -----` `protect against invalid tcp attack On`

Related Commands	**Command**	**Description**
	ip deny invalid-tcp	Enables the anti-attack of the invalid TCP packets.
Platform Description	N/A	

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 Examples	The following example displays the anti-land-attack state. `Ruijie# show ip deny land` `DoS Protection Mode State` `------------------------------ -----` `protect against land attack On`	

Related Commands	Command	Description
	no ip deny land	Enables the anti-land-attack function.
Platform Description	N/A	

ACL & QoS Configuration Commands

1 ACL Commands

1.1 Command ID table

For IDs used in the following commands, refer to the command ID table below:

ID	Meaning
ID	Number of access list. Range: Standard IP ACL: 1 to 99, 1300 to 1999 Extended IP ACL: 100 to 199,2000 to 2699 Extended MAC ACL: 700 to 799 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 *idx*	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 tm-rng-name	Time range of packet filtering, named *tm-rng-name*
tos	Type of service (0 to 15)
cos	Class of service (0-7)
cos inner *cos*	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) *port* 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 *tcpf*	Match all bits of the TCP flag.
established	Match the RST or ACK bit of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{rule mask offset}$^{+}$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table "+" sign indicates at least one group
log	Output the matching syslog when the packet matches the ACL rule.

The fields in the packet are as follows:

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

The corresponding offset table is as follows:

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	Resrved 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.

1. 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**]

2. 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**]

3. 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*]]

4. 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*][**inne**r *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 None

Command Mode Global configuration 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 Examples

1. Example of the standard IP ACL

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
id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
text	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 *id*	Displays the access list of a specified number, including the remarks for the access list.
show access-lists *name*	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
id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
text	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 Examples The following example writes a comment for an entry in ACL102.

```
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 *id*	Displays the access list of a specified number, including the remarks for the access list entry.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list entry.

Platform Description

1.5 clear counters access-list

Use this command to clear counters of packets matching ACLs.

clear counters access-list [*id* | *name*]

Parameter Description

Parameter	Description

id	Access list number
name	Access list name

Defaults

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the counters of packets matching the specified or all ACLs.

Configuration Examples The following example clears the packet matching counter of ACL No. 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  (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 Description N/A

1.6 clear access-list counters

Use this command to clear counters of packets matching the deny entries in ACLs.

clear access-list counters [*id* | *name*]

Parameter Description

Parameter	Description
id	Access list number
name	Access list name

Defaults

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the counters of packets matching the deny entries in ACLs.

Configuration Examples The following example clears the packet matching counter of ACL No. 1:

Before configuration:

```
Ruijie #show access-lists
ip access-list standard 1
   10 deny host 50.1.1.2 (10 matches)
   20 permit host 60.1.1.2 (15 matches)
   (10 packets filtered)
```

After configuration:

```
Ruijie# end
Ruijie# clear access-list counters
Ruijie# show access-lists
ip access-list standard 1
   10 deny host 50.1.1.2 (10 matches)
   20 permit host 60.1.1.2 (15 matches)
```

Related Commands

Command	Description
expert access-list	Defines an expert ACL.
deny	Defines a deny ACL entry.
permit	Defines a permits ACL entry.

Platform Description N/A

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.

5. Standard IP ACL

[*sn*] **deny** {*source source-wildcard* | **host** *source* | **any| interface** *idx* }[**time-range** *tm-range-name*] [**log**]

6. 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*]

7. Extended MAC ACL

[*sn*] **deny** { **any** | **host** *source-mac-address* } { **any** | **host** *destination-mac-address* } [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]

8. 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** } {*destinationdestination-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
sn	ACL entry sequence number
source-ipv6-prefix	Source IPv6 network address or network type
destination-ipv6-prefix	Destination IPv6 network address or network type
prefix-length	Prefix mask length
source-ipv6-address	Source IPv6 address
destination-ipv6-address	Destination IPv6 address
dscp	Differential Service Code Point
dscp	Code value, within the range of 0 to 63
flow-label	Flow label
flow-label	Flow label value, within the range of 0 to 1048575.
protocol	For the IPv6, the field can be ipv6 | icmp | tcp | udp and number in the

	range 0 to 255
time-range	Time range of the packet filtering
time-range-name	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 Description N/A

1.8 expert access-group

Use this command to apply the specified expert access list 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
id	Expert access list number: 2700 to 2899
name	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 on the interface.

Command mode Interface configuration mode.

Usage Guide This command is used to apply the specified access list on the interface to control the input and output data streams on the interface. 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
name	Name of the advanced expert access list

Defaults None

Command mode Global configuration mode

Usage Guide Use this command to create an advanced expert access list (namely, ACL80) to match your custom fields.

Configuration Examples The following example creates an advanced expert access list named adv-acl.

```
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 *name*	Displays the access list of a specified name.

Platform Description N/A

1.10 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
id	Extended expert access list number: 2700 to 2899
name	Name of the extended expert access list

Defaults None

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
show access-lists	Displays the extended expert ACLs

Platform Description N/A

1.11 expert access-list 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
id	Expert access list number: 2700 to 2899.
name	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 Description N/A

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
id	Expert access list number: 2700 to 2899.
name	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

Command	Description

Commands		
	-	-

Platform Description N/A

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
Id	Expert access list number: 2700 to 2899.
name	Name of the expert access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	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”:

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 access list on the interface. Use the **no** form of this command to remove the global 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 access list is applied on the interface.

Command mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example applies the global 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 to an interface. Use the **no** form of this command to remove the access list from the interface.

ip access-group {*id* | *name*} {**in** | **out**}

no ip access-group { *id* | *name*} {**in** | **out**}

Parameter Description

Parameter	Description
id	IP access list or extended IP access list number: 1 to 199, 1300 to 2699
name	Name of the IP ACL
in	Filters the incoming packets of the interface.
out	Filters the outgoing packets of the interface.

Defaults No access list is applied on the interface by default.

Command mode Interface configuration mode.

Usage Guide Use this command to control access to a specified interface.

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 Description N/A

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
id	Access list number: Standard: 1 to 99, 1300 to 1999; Extended: 100 to 199, 2000 to 2699.
name	Name of the access list

Defaults None

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 Examples 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 Description N/A

1.17 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
time	For the access rule with the **log** 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 Examples The following example configures the interval for the IPv4 access list log update to 10 minutes:

```
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 **deny** access entries.
permit	Defines the **permit** access entries.
show running	Displays running configurations of the device.

Platform Description N/A

1.18 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
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	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 Examples 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 Description N/A

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
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	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 Description N/A

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
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the standard or extended IP access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	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 ACL1:

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 Description N/A

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
name	Name of the IPv6 access list.

Defaults None

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 Description N/A

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
name	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
time	For the access rule with the **logging** 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 **deny** access entries.
permit	Defines the **permit** 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
name	Name of the IPv6 access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	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 IPv6 access list “v6-acl”:
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 Description N/A

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.
ipv6 traffic-filter *name* { **in** | **out** }

no ipv6 traffic-filter *name* { **in** | **out** }

Parameter Description

Parameter	Description
name	Name of IPv6 access list
in	Specifies filtering on inbound packets
out	Specifies filtering on outbound packets

Defaults None

Command mode Interface configuration mode.

Usage Guide Use this command to apply the IPv6 access list to an 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 Description N/A

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
text	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 Description N/A

1.27 mac access-group

Use this command to apply the specified MAC access list 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
id	MAC access list number. The range is from 700 to 799.
name	Name of the MAC access list
in	Specifies filtering on the inbound packets.
out	Specifies filtering on the outbound packets.

Defaults None

Command mode Interface configuration mode.

Usage Guide Use this command to apply the access list to the interface 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 Description N/A

1.28 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
id	Extended MAC access list number. The range is from 700 to 799.
name	Name of the extended MAC access list

Defaults None

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 Examples The following command creates an extended MAC access list named mac-acl:

```
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 Description N/A

1.29 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
id	Extended MAC access list number. The range is from 700 to 799.
name	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

1.30 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
id	Extended MAC access list number: 700 to 799.
name	Name of the extended MAC access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	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”:

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.

9. Standard IP ACL

[*sn*] **permit** {*source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*] [**log**]

10. 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*]

11. 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*]]

12. 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**}
13. 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.
ipv6 traffic-filter	Applies the extended IPv6 access list to the interface.
ip access-group	Applies the IP access list to the interface.
mac access-group	Applies the extended MAC access list to the interface.
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Define an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.
deny	Defines the **deny** access entry.

Platform Description N/A

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
interface-name	Redirect interface
id	Access list number
name	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 Examples The following example configures access redirection.

```
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 Description N/A

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

Parameter	Description

Description

text	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 Examples The following example writes remarks for the entry in extended IP access list 102.

```
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.
ip access-list	Defines an IP access list.

Platform Description N/A

1.34 security access-group

Use this command to configure a interface secure channel.
security access-group { *id* | *name* }
no security access-group

Parameter Description

Parameter	Description
id	Access list number.
name	Name of the access list.

Defaults None

Command Interface configuration mode

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 Examples The following example configures a secure channel on interface GigaEthernet 1/1.

```
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 Description N/A

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
id	Access list number.
name	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 Description N/A

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 used this command to configure the interface as exceptional.

Configuration Examples The following example configures interface GigaEthernet 1/1 as an exceptional interface of the secure channel.

```
Ruijie(config)# interface GigaEthernet 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*]

Parameter Description

Parameter	Description
interface	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
Applied On interface GigabitEthernet 0/8.
```

Related Commands

Command	Description
ip access-group	Applies the IP access list to the interface.
mac access-group	Applies the MAC access list to the interface.
expert access-group	Applies the expert access list to the interface.
ipv6 traffic-filter	Applies the IPv6 access list to the interface.

Platform Description N/A

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
id	Access list number
name	Name of the IP access list
summary	Access list summary

Defaults N/A

Command Global configuration mode

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)
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Defines an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.

Platform Description N/A

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*]

Parameter Description

Parameter	Description
interface	Interface name

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 Commands

Command	Description
expert access-list	Defines an extended 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 Description

Parameter	Description
interface	Interface name

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.
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.

Platform Description N/A

1.41 show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.

show ipv6 traffic-filter [**interface** *interface*]

Parameter Description

Parameter	Description
interface	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.
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.

Platform Description N/A

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
interface	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.
```

Related Commands

Command	Description
mac access-list	Defines a MAC access list.

Platform Description N/A

1.43 show redirect interface

Use this command to display the access redirection configuration.
show redirect [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	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 Examples The following example displays the access redirection configuration on interface GigabitEthernet 0/3.

```
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 Examples The following example enables the SVI filter only for the Layer3 packets.

```
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 a class from the policy map.

class *class-map-name*

no class *class-map-name*

Parameter Description

Parameter	Description
class-map-name	Reference to a class map.

Defaults None

Command Mode Policy configuration mode

Usage Guide N/A

Configuration Examples The following example adds reference to the class map named cmap1.

```
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
show policy-map [*policy-map-name* **[class** *class-map-name*]]	Displays the policy map.

Platform Description N/A

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 Description

Parameter	Description
class-map-name	Class map name. The class map name can be a maximum of 31 characters.

Defaults None

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example creates a class map named cm_acl to match an access list named me.

```
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
```

Related Commands

Command	Description
show class-map [*class-map-name*]	Displays the class map.

Platform Description N/A

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

Description	*weight1...weight8*	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 N/A

Configuration Examples The following example configures the DRR queue weight ratio to 1:1:1:2:2:4:6:8.

```
Ruijie(config)# drr-queue bandwidth 1 2 3 4 5 6 7 8
```

Related Commands

Command	Description
show mls qos queuing	Displays information about the queue.

Platform Description N/A

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 Description

Parameter	Description
access-group *access_list*	Identifies a numbered or named access list as the match criteria.
ip dscp *dscp-vlaue-list*	Identifies DSCP values as the match criteria. Multiple DSCP can be configured. The range is from 0 to 63.
ip precedence *pre-vlaue-list*	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 Examples The following example creates a class map named cmap1 to match DSCP 20, 22, 24 and 30.

```
Ruijie(config)# class-map cmap1
Ruijie(config-cmap)# match ip dscp 20 22 24 30
```

Related Commands

Command	Description
show class-map [*class-map-name*]	Displays the class map.

Platform Description N/A

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 Description

Parameter	Description
default-cos	CoS value of the interface. The range is from 0 to 7.

Defaults The default CoS value is 0.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the default CoS value to 7.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mls qos cos 7
```

Related Commands

Command	Description
show mls qos interface *interface-id*	Displays information of the specified interface.

Platform Description N/A

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 Description

Parameter	Description
dscp1...dscp8	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
show mls qos maps cos-dscp	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 Description

Parameter	Description
dscp-list	DSCP list. The range is from 0 to 63.
cos	CoS value. The range is from 0 to 7.

Defaults The default DSCP-CoS mapping is listed below:

DSCP 0-7	DSCP 8-15	DSCP 16-23	DSCP 24-31	DSCP 32-39	DSCP 40-47	DSCP 48-55	DSCP 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
show mls qos maps dscp-cos	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
dscp1...dscp8	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
show mls qos maps ip-pre-dscp	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**]

no mls qos scheduler

Parameter Description

Parameter	Description
sp	Specifies the absolute priority scheduling.
rr	Specifies the round-robin scheduling.
wrr	Specifies the frame count weighted round-robin scheduling.
drr	Specifies the frame length weighted round-robin scheduling.

Defaults The default queue scheduling is **wrr**.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies the sp scheduling.

```
Ruijie(config)# mls qos scheduler sp
```

Related Commands

Command	Description
show mls qos scheduler	Displays the output queue scheduling.

Platform Description N/A

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 Description

Parameter	Description
cos	Specifies the CoS trust mode.
dscp	Specifies the DSCP trust mode.
ip-precedence	Specifies the IP-PRE trust mode.

Defaults No trust mode is configured by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the CoS trust mode.

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mls qos trust cos
```

Related Commands

Command	Description
show mls qos interface *interface-id*	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

Parameter Description

Parameter	Description
rate-bps	Bandwidth limit value per second (The unit is KBits). This value depends on the specific product.
burst-byte	Burst traffic limit value (The unit is KBytes). This value depends on the specific product.
drop	Drops the packet. This is available only when the packet exceeds the bandwidth limit.
dscp *new-dscp*	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.
cos *new-cos*	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.
none-tos	Modifies the CoS value only.

Defaults No traffic policing is configured for the class map by default.

Command Mode Policy map class configuration mode

Usage Guide N/A

Configuration Examples The following example configures traffic policing which modifies the DSCP value of the packet to 6 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
show policy-map [*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration.

Platform Description N/A

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 Description

Parameter	Description
policy-map-name	Policy map name. The policy map name can be a maximum of 31 characters.

Defaults No policy map is configured by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example creates policy map “po”, and then adds a reference to class map “cmap1”.

```
Ruijie(config)# policy-map po
Ruijie(config-pmap)# class cmapl
```

Related Commands

Command	Description
show policy-map [*policy-map-name* [**class** *class-map-name*]]	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 Description

Parameter	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 Commands

Command	Description
show mls qos scheduler	Displays the output queue scheduling policy.

Platform Description N/A

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.

priority-queue cos-map *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]

no priority-queue cos-map

default priority-queue cos-map

Parameter Description

Parameter	Description
qid	Queue ID. The range is from 1 to 8.
cos0 ... cos7	CoS value. The range is from 0 to 7.

Defaults The default mapping between the CoS value and the queue ID is listed below:

Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7	Queue 8

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 The following example maps the CoS 3, 5 to the output queue 1.

```
Ruijie(config)#priority-queue cos-map 1 3 5
```

Related Commands

Command	Description
show mls qos queuing	Displays the output queues.

Platform Description N/A

2.15 qos queue

Use this command to configure a minimum or maximum of the interface bandwidth to a queue. Use the **no** or **default** form of this command to remove the minimum or maximum of the interface bandwidth.

qos queue [**ucast** | **mcast**] *queue-id* **bandwidth** { **minimum** | **maximum** } *bandwidth*

no qos queue [**ucast** | **mcast**] *queue-id* **bandwidth** { **minimum** | **maximum** }

default qos queue [**ucast** | **mcast**] *queue-id* **bandwidth** { **minimum** | **maximum** }

Parameter Description

Parameter	Description
queue [**ucast** | **mcast**]	The **queue ucast** keyword indicates configuring the minimum or maximum of the interface bandwidth to the unicast queue on the device supporting the unicast queue bandwidth configuration. The **queue mcast** keyword indicates configuring the minimum or maximum of the interface bandwidth to the multicast queue on the device supporting the multicast queue bandwidth configuration. The **queue** keyword indicates configuring the minimum or maximum of the interface bandwidth to the queue on the device supporting both unicast and multicast queue bandwidth configuration.
queue-id	Queue ID. The range is from 1 to 8.
bandwidth { **minimum** | **maximum** } *bandwidth*	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 Interface configuration mode

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
show qos bandwidth [**interfaces** *interface-id*]	Displays the interface bandwidth of the queue.

Platform Description N/A

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 Description

Parameter	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 Description N/A

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 Description

Parameter	Description
input	Configures input rate limiting.
output	Configures output rate limiting.
bps	Bandwidth limit value per second (The unit is KBits). This value depends on the specific product.
burst-size	Burst traffic limit value (The unit is KBytes). This value depends on the specific product.

Defaults Rate limiting is not configured by default.

Command Mode Interface configuration 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
	show mls qos rate-limit [**interface** *interface-id*]	Displays the rate limiting configuration of the interface.

Platform Description N/A

2.18 service-policy

Use this command to apply the policy map to the interface or the virtual group. Use the **no** or **default** form of this command to remove the policy map from the interface or the virtual group.

service-policy { **input** | **output** } *policy-map-name*

no service-policy { **input** | **output** } *policy-map-name*

default service-policy { **input** | **output** } *policy-map-name*

Parameter Description	Parameter	Description
	policy-map-name	Policy map name
	input	Applies the policy map to the input direction.
	output	Applies the policy map to the output direction.

Defaults No policy map is configured on the interface or virtual group by default.

Command Mode Interface configuration mode, and virtual group configuration mode.

Usage Guide N/A

Configuration Examples The following example applies policy map “po” to the input direction of interface GigabitEthernet 1/3.

```
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
	show mls qos interface policers	Displays the policy map configuration on the interface.
	show mls qos virtual-group policers	Displays the policy map configuration on the virtual group.

Platform Description N/A

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 value from the traffic.

set { **ip dscp** *new-dscp* | **cos** *new-cos* [**none-tos**] }

no set { **ip dscp** | **cos** | **vid** }

Parameter Description

Parameter	Description
ip dscp *new-dscp*	Configures the DSCP value for the traffic. The range is from 0 to 63.
cos *new-cos*	Configures the CoS value for the traffic. The range is from 0 to 7.
none-tos	Configures the CoS value only.

Defaults No CoS or DSCP value is configured for the traffic in policy map class mode.

Command Mode Policy map class configuration mode

Usage Guide N/A

Configuration Examples The following example creates policy map “pmap1”, and adds a reference to class map “cmap1”.

```
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
show policy-map[*policy-map-name* [**class** *class-map-name*]]	Displays the policy map configuration on the interface.

Platform Description N/A

2.20 show class-map

Use this command to display the class map.

show class-map [*class-map-name*]

Parameter Description

Parameter	Description
class-map-name	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.

```
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 Description N/A

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 Description

Parameter	Description
interface-id	Interface name
policers	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 GigabitEthernt 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
```

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 Description N/A

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 Description

Parameter	Description
cos-dscp	Displays the CoS-DSCP mapping.
dscp-cos	Displays the DSCP-CoS mapping.
ip-prec-dscp	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 Description N/A

2.23 show mls qos queuing

Use this command to display the QoS queuing configuration.

show mls qos queuing

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 QoS queuing configuration.

```
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

drr bandwidth weights:
qid weights
--- -------
1   3
2   3
3   3
4   3
5   3
6   3
7   3
8   3
```

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.
cos	Indicates the CoS value.
qid	Indicates the queue ID.
weights	Indicates the weight value

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 Description

Parameter	Description
interface-id	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

Command	Description

Commands	N/A	N/A

Platform Description N/A

2.25 show mls qos scheduler

Use this command to display the queue scheduling policy.

show mls qos scheduler

Parameter Description

Parameter	Description
N/A	N/A

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
```

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. The other queue scheduling policies are listed as follows: SP: Strict Priority RR: Round Robin DRR: Deficit Round Robin

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 Description

Parameter	Description
virtual-group-number	Virtual group number. The range is from 1 to 128.
policers	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 Description

Parameter	Description
policy-map-name	Policy map name
class-map-name	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 Description	**Parameter**	**Description**
	interface-id	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 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 Total ucast-queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when only unicast queue is displayed.
Total mcast-queue minimum-bandwidth Total mcast-queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when only multicast queue is displayed.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.29 show queueing wred interface

Use this command to display WRED settings on the interface.

show queueing wred interface *interface-id*

Parameter Description

Parameter	Description
interface-id	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
virtual-group-number	Virtual group number. The range is from 1 to 128.
summary	Displays the member port in all virtual groups.

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 member port in all virtual groups.

```
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
virtual-group-number	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
show virtual-group [*virtual-group-number* | **summary**]	Displays the virtual group configuration.

Platform Description N/A

2.32 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

Parameter	Description

Description	*weight1...weight8*	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 Examples The following example configures the WRR queue weight ratio to 1:1:1:1:2:2:4:8.

```
Ruijie(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
```

Related Commands	**Command**	**Description**
	show mls qos queuing	Displays the QoS queuing configuration.

Platform Description N/A

2.33 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**
	threshold_id	Threshold number. The range is from 1 to 2. Up to two threshold values can be configured.
	cos_N	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
show queueing wred interface *interface-id*	Displays the WRED configuration on the interface.

Platform Description N/A.

2.34 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
queue_id	Queue ID.
thrN	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

show queueing wred interface *interface-id*	Displays the WRED configuration on the interface.

Platform Description N/A.

2.35 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
queue_id	Queue ID.
proN	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 Examples The following example configures the WRED packet drop values to 50 and 70 for queue 1.

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# wrr-queue random-detect probability 1
50 70
```

Related Commands

Command	Description
show queueing wred interface *interface-id*	Displays the WRED configuration on the interface.

Platform Description N/A.

Reliability Configuration Commands

1 RLDP Commands

1.1 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
interval	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
rldp detect-max	Sets the maximum number of detections.

Platform Description N/A.

1.2 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

num	Maximum number of detections in the range 2 to 10

Defaults 2.

Command Mode Global configuration mode.

Usage Guide This command is used together with the detection interval to specify the maximum number of detections.

Configuration Examples The following example shows how to set the maximum number of detections as 5:

```
Ruijie(config)# rldp detect-max 5
```

Related Commands

Command	Description
rldp detect-interval	Sets the detection interval.

Platform Description N/A.

1.3 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 Mode Global configuration mode.

Usage Guide You can enable RLDP on the interface only when the global RLDP is enabled.

Configuration Examples The following example shows how to enable RLDP:

```
Ruijie(config)# rldp enable
```

Related Commands

Command	Description
rldp port	Enables the RLDP function on the port.

Platform Description N/A.

1.4 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 Mode Global configuration 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 Examples The following example shows how to enable RLDP neighbor negotiation:

```
Ruijie#config
Ruijie(config)#rldp neighbor-negotiation
```

Related Commands

Command	Description
rldp port	Enables the RLDP function on the port.

Platform Description N/A.

1.5 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
unidirection-detect	Sets unidirectional link detection.
bidirection-detect	Sets bidirectional link detection.
loop-detect	Sets loop detection type.
warning	Warns the user.
shutdown-svi	Shutdowns the SVI the port belongs to.
shutdown-port	Shutdowns 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
rldp enable	Enables RLDP globally.

Platform Description N/A.

1.6 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 Examples The example below demonstrates how to use this command:

```
Ruijie# rldp reset
```

Related Commands

Command	Description
rldp enable	Enables RLDP globally.

Platform Description N/A.

1.7 show rldp

Use this command to display the RLDP information.

show rldp [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface ID

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples N/A.

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A.

2 DLDP Commands

2.1 clear dldp

Use this command to clear statistics about the number of times that DLDP is down or up at a specified monitoring point for renewing statistics.

clear dldp [**interface** *interface-name* [*ip-address*]]

Parameter Description

Parameter	Description
interface-name	Name of an L3 interface
ip-address	IP address of a peer device

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide DLDP records statistics about the number of times that DLDP is down or up. You can use this command to clear statistics about the number of 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 number of 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 number of 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 number of times that DLDP is down or up at all monitoring points on all interfaces.

```
Ruijie#clear dldp
```

The following example clears statistics about the number of 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 number of 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

2.2 dldp

Use this command to enable DLDP detection. Use the **no** form of this command to restore the default setting.

dldp *ip-address* [**next-hop** *ip-address*] [**interval** *tick* | **retry** *retry-num* | **resume** *resume-num*]

no dldp *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address of the peer device to be detected
next-hop *ip-address*	Next-hop IP address specified when the device to be detected belongs to another different network
interval *tick*	Detection interval. The value range is from 1 to 6000 in the unit of ticks, where 1 tick is equal to 10 milliseconds. The value must be an integral multiple of five.
retry *retry-num*	Number of retry times. The value range is from 1 to 3600.
resume *resume-num*	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

The value of *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.

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 next-hop 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

2.3 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 Description	Parameter	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.

Configuration Examples The following example sets DLDP to the passive mode.

```
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

2.4 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
tick	Detection interval (in ticks), in the range from 5 to 6000. The value must be a multiple of 5. (1tick = 10 milliseconds)

Defaults The default is 10.

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

2.5 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

Parameter Description

Parameter	Description
retry-num	Retry count, in the range from 1 to 3600.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide This command is used to set the DLDP retry count.

Configuration Examples The following example sets the DLDP retry count to 4.

```
Ruijie#config
Ruijie(config)#dldp retry 4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.6 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

Parameter Description

Parameter	Description
resume-num	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.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide This command is used to set the DLDP recovery count.

Configuration Examples The following example sets the DLDP recovery count to 4.

```
Ruijie#config
Ruijie(config)#dldp resume 4
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.7 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
interface-name	Name of an L3 interface
statistic	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 L3 interface. If an L3 interface is specified, this command displays DLDP configuration and statistics at all monitoring points on the L3 interface.

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
---------  -------  -----------  -----------  --------  -----  ------
------
Vl2       Passive  192.168.6.3  192.168.2.2  10       5     3      Up
Vl3       Passive  192.168.7.3            10       5     3      Up
Vl4       Passive  192.168.3.3  192.168.4.2  10       5     3      Up
```

Configuration Examples The following example displays DLDP configuration information at all monitoring points on the L3 interface *vlan 2.*

```
Ruijie#show dldp intface vlan2
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------
------
Vl2       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
---------  -------  -----------  -----------  --------  ----------
```

```
Vl2       Passive  192.168.6.3  2h34m5s     10       9
Vl4       Passive  192.168.3.3  1d2h3m52s    10       9
```

The following example displays DLDP statistics at all monitoring points on the L3 interface *vlan 2*.

```
Ruijie#show dldp statistic interface vlan 2
Interface  Type        Ip      record-time  Up-count  Down-count
---------  -------  -----------  -----------  --------  ----------
Vl2       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: y: year d: day h: hour m: minute s: second Using the *Up-count* and *Down-count* 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

3 VRRP Commands

3.1 show vrrp

Use this command to display the VRRP information.

show vrrp [**brief** | *group*]

Parameter Description

Parameter	Description
brief	(Optional) Displays the brief of the VRRP group.
group	Number of the VRRP group to be displayed

Defaults N/A

Command Mode Privileged EXEC 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 Time  Own Pre State   Master addr   Group addr
FastEthernet 0/0  1  100   -  -  P  Backup  192.168.201.213 192.168.201.1
FastEthernet 0/0   2   120  -   -  P  Master  192.168.201.217 192.168.201.2
Ruijie#
```

Related Commands

Command	Description
Ruijie config-if # **vrrp** *group ip ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.

Platform Description N/A

3.2 show vrrp interface

Use this command to display the information of the VRRP on the interface.

show vrrp interface *type number* [**brief**]

Parameter Description

Parameter	Description
type	Interface type
number	Interface number
brief	(Optional) Displays the brief of the VRRP group on the interface.

Defaults N/A

Command Mode Privileged EXEC 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 Commands

Command	Description
Ruijie config-if # **vrrp** *group* **ip** *ip address* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device

Platform Description N/A

3.3 show vrrp packets statistics

Use this command to displays the statistics of the VRRP packets transmission.

show vrrp packet statistics [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and number.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the statistics of VRRP packets transmitting on all interfaces.

```
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 Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.4 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 Description	Parameter	Description
	group	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 Examples The following example enables the accept mode on the group 1:

```
vrrp ipv6 1 accept_mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 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 Description

Parameter	Description
group	VRRP group number
string	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 Examples The following example sets the authentication password for VRRP group 1.

```
vrrp 1 authentication x30dn78k
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 vrrp bfd (global configuration mode)

Use this command to enable the global BFD correlation for theIPv4 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 Description

Parameter	Description
interface-type interface-number	Interface type and interface number
ip-address	Neighbor IP address

Defaults By default, the global BFD correlation for IPv4 VRRP is disabled.

Command Mode Global configuration mode

Usage Guide

1. After the global BFD correlation for IPv4 VRRP is configured, the BFD correlation configuration for the IPv4 VRRP groups will be removed.
2. The global BFD correlation for IPv4 VRRP configured later will override the earlier configuration.
3. The IP address and BFD session of the interface must be configured before configuring the **vrrp bfd** command.
4. The global IPv4 VRRP BFD session applies to the IPv4 VRRP router which is consists of two devices only.

Configuration Examples The following example enables global BFD correlation for IPv4 VRRP.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 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

Description		
	group	VRRP group ID
	ip-address	Neighbor IP address

Defaults By default, no BFD correlation is configured for the IPv4 VRRP group on the interface.

Command Mode Interface configuration mode.

Usage Guide
1. After the global BFD correlation for IPv4 VRRP is configured, the BFD correlation configuration for the IPv4 VRRP groups will be removed.
2. The IP address and BFD session of the interface must be configured before configuring the **vrrp bfd** command.

Configuration Examples The following example enables BFD correlation for the VRRP group.

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 Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.8 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 Description	Parameter	Description
	min-seconds	When the interface is up, VRRP group shall be reloaded after at least

	min-seconds.
reload-seconds	The reload latency of the VRRP group. If the configured min-seconds is more than reload-seconds, the actual reload latency of the VRRP group will be min-seconds.

Defaults This function is disabled by default.

Command Mode Interface configuration 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 0-60.

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.

```
interface FastEthernet 0/0
shutdown
ip address 10.0.1.1 255.255.255.0
vrrp delay minimum 10
vrrp 1 ip 10.0.1.20
no shutdown
show vrrp 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.9 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 *group* **description** *text*

no vrrp *group* **description**

Parameter Description

Parameter	Description
group	VRRP group number
text	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 Mode Interface configuration 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.

```
interface FastEthernet 0/0
ip address 10.0.1.1 255.255.255.0
vrrp 1 ip 10.0.1.20
vrrp 1 description "Building A - Marketing and Administration"
```

Related Commands

Command	Description
Ruijie(config-if)# **vrrp** *group* ip *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device

Platform Description N/A

3.10 vrrp detection-vlan

Use this command to enable IPv4 VRRP packets to be sent to only the first 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
no vrrp detection-vlan

Parameter Description

Parameter	Description
first-subvlan	IPv4 VRRP packets are sent to only the first 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 two modes in which IPv4 VRRP packets are sent to a Super VLAN interface: to only the first Sub VLAN or to 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.

Examples

```
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
vrrp ip	Enables the VRRP function and set the IP address of the VRRP.

Platform Description N/A

3.11 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 Description

Parameter	Description
group	VRRP group number of the virtual device
ipaddress	IP address of the virtual device
secondary	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.

```
interface FastEthernet 0/0
no switchport// Used on the switch only.
ip address 10.0.1.1 255.255.255.0
```

```
ip address 10.0.2.1 255.255.255.0 secondary
vrrp 1 ip 10.0.1.20
vrrp 1 ip 10.0.2.20 secondary
```

Related Commands

Command	Description
Ruijie# show vrrp [brief | group]	Displays the VRRP configuration.

Platform Description N/A

3.12 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
group	VRRP group number of the virtual device.
ipv6-address	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 1and virtual IPv6 address FE80::1 and 2001::1.

```
interface FastEthernet 0/0
no switchport
ipv6 enable
ip6 address 2001::2/64
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2001::1
```

Related Commands

Command	Description
Ruijie# **show ipv6 vrrp** [**brief | group**]	Displays the IPv6 VRRP configuration.

Platform N/A

Description

3.13 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 *group* **preempt** [**delay** *seconds*]

no vrrp *group* **preempt** [**delay**]

Parameter Description

Parameter	Description
group	VRRP group number
delay *seconds*	(Optional)Specifies the delay before a device declares itself master. 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
// 'no switchport'
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
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
```

```
// 'no switchport'
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
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
Ruijie config-if # **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
Ruijie config-if # **vrrp** *group* **priority** *level*	Sets the VRRP group priority.

Platform Description N/A

3.14 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 *group* **priority**

Parameter Description

Parameter	Description
group	VRRP group number
level	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 Mode Interface configuration mode.

Usage Guide None.

Configuration Examples The following example following example sets the priority of VRRP group 1 as 254.

```
vrrp 1 priority 254
```

Related Commands

Command	Description
Ruijie config-if # **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
Ruijie(config-if)# **vrrp** *group* **preempt** [**delay**	Sets the VRRP in the preemption mode.

seconds]	

Platform Description N/A

3.15 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 Description

Parameter	Description
group	VRRP group number
advertise-interval	Sets the interval time in seconds between sending VRRP advertisement.
csec *centisecond-interval*	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. 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 Mode Interface configuration 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 Examples The following example sets the VRRP advertisement interval as 4 seconds.

```
vrrp 1 timers advertise 4
```

Related Commands

Command	Description
Ruijie config-if # **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
Ruijie config-if # **vrrp group timers learn**	Enables the timer learning function.

Platform Description N/A

3.16 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 *group* **timers learn**

no vrrp *group* **timers learn**

Parameter Description

Parameter	Description
group	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.

```
vrrp 1 timers learn
```

The following example to enables the timer learning function on the IPv6 VRRP group 1.

```
vrrp ipv6 1 timers learn
```

Related Commands

Command	Description
Ruijie config-if # **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
Ruijie config-if # **vrrp** *group* **ipv6** *ipaddress*	Enables the VRRP function and set the IPv6 address for the virtual device.
Ruijie config-if # **vrrp** *group* **timers advertise** *interval*	Sets the IPv4 VRRP advertising interval.
Ruijie config-if # **vrrp ipv6** *group* **timers advertise** *interval*	Sets the IPv6 VRRP advertising interval.

Platform Description N/A

3.17 vrrp track

Use the **vrrp** *group* **track** *interface-type number* command to enable the VRRP track in the interface

configuration mode. Use the **vrrp** *group* **track** *ip_address* command to enable the VRRP IP address track. Use the **vrrp** *group* **track bfd** command to track the specified neighbor IP address via BFD. Use the **no** form of this command to restore the default setting.

vrrp *group* **track** { *interface-type number* | **bfd** *interface-type number ipv4-address* } [*priority*]

vrrp *group* **track** *ip-address* [[[**interval** *interval-value*] **timeout** *timeout-value*] *priority*]

vrrp *group* **track** [*interface-type number* | **bfd** *interface-type number ipv4-address*] [*ip-address*]

Parameter Description

Parameter	Description
group	VRRP group number
interface-type	Type of monitored interface
number	Number of the monitored interface
Ipv4-*address*	Monitored IPv4 address. With BFD configured, it refers to the neighbor IP address.
interval-value	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 3s.
timeout-value	The timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1s.
interface-priority	VRRP priority change range when the interface or ip address reachability status changes. If this parameter is not selected, the default value is 10.

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). This command can also be used to monitor the reachability of the specified IP address.

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.

```
vrrp 1 track FastEthernet 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
Ruijie config-if # **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
Ruijie config-if # **vrrp** *group* **priority** *level*	Sets the VRRP group priority.

Platform Description N/A

3.18 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.

vrrp *group* **version** { **2** | **3** }

no vrrp *group* **version**

Parameter Description

Parameter	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 gig4/1.

```
vrrp 1 version 3
```

Related Commands

Command	Description
Ruijie config-if # **vrrp** *group* **ip** *ipaddress*	Enables the VRRP function and set the IP

[**secondary**]	address for the virtual device.
Ruijie config-if # **vrrp** *group* **timers advertise** *interval*	Sets the interval of sending the VRRP advertisement.

Platform Description N/A

4 VRRP Plus Commands

4.1 show vrrp balance

Use this command to display the VRRP Plus brief or details.

show vrrp balance [**brief** | *group*]

Parameter Description

Parameter	Description
brief	(Optional) Displays the VRRP Plus brief.
group	(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
vrrp *group* **balance**	Enables the VRRP Plus function.
vrrp *group* **load-balancing { host-dependent | round-robin | weighted }**	Sets the load balancing policy of the VRRP Plus.
show vrrp balance interface *type number* **[brief]**	Displays the VRRP Plus running status of the specified interface.

Platform Description N/A.

4.2 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
interface type number	Specifies the interface type and number.
brief	(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
vrrp *group* **balance**	Enables the VRRP Plus function.
vrrp *group* **load-balancing { host-dependent | round-robin | weighted }**	Sets the load balancing policy of the VRRP Plus.
s**how vrrp balance interface** *type number* **[brief]**	Displays the VRRP Plus running status of the specified interface.

Platform Description N/A.

4.3 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
group	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 N/A

Configuration Examples The following example enables the VRRP Plus function on the Layer3 interface FastEthernet0/0.

```
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
vrrp load-balancing	Sets the load balancing policy of the VRRP

	Plus.
show vrrp balance	Displays the VRRP Plus running status.
show vrrp balance interface	Displays the VRRP Plus running status of the specified interface.

Platform Description N/A.

4.4 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
group	VRRP group number. The range is from 1 to 255.

Defaults By default, forwarding preemption is enabled.

Command Mode Interface configuration mode

Usage Guide The VRRP Plus function should be configured before enabling forwarding preemption.

Configuration Examples The following example enables the forwarding preemption function of the VRRP Plus backup group on the Layer3 interface FastEthernet0/0.

```
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
vrrp *group* **balance**	Enables the VRRP Plus function.
show vrrp balance [brief | *group*]	Displays the VRRP Plus running status.
show vrrp balance interface *type number* **[brief]**	Displays the VRRP Plus running status of the specified interface.

Platform N/A.

Description

4.5 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
group	Specifies the VRRP group ID.
host-dependent	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.
round-robin	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.
weighted	Sets the weight balancing policy, so as to perform the ARP reply based on the device weight of the backup group.

Defaults Round-robin.

Command Mode Interface configuration mode.

Usage Guide The VRRP Plus function should be enabled before setting the VRRP Plus load balancing policy.

Configuration Examples The following example sets the load balancing policy of the VRRP Plus group1 as host-dependent.

```
Ruijie(config-if)# vrrp 1 ip 192.168.1.1
Ruijie(config-if)# vrrp 1 balance
Ruijie(config-if)# vrrp 1 load-balancing host-dependent
```

Related Commands

Command	Description
vrrp *group* **balance**	Enables the VRRP Plus function.
show vrrp balance [brief | *group*]	Displays the VRRP Plus running status.
s**how vrrp balance interface** *type number* **[brief]**	Displays the VRRP Plus running status o the specified interface.

Platform Description N/A.

4.6 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
group	VRRP Plus backup group ID, in the range of 1 to 255.
redirect	The redirection time, 300 seconds (namely 5 minutes) by default, in the range of 0 to 3,600.
timeout	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 Mode Interface configuration 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-if)# vrrp 1 ip 192.168.1.1
Ruijie(config-if)# vrrp 1 balance
Ruijie(config-if)# vrrp 1 timers redirect 300 6000
```

Related Commands

Command	Description
vrrp *group* **balance**	Enables the VRRP Plus function.
show vrrp balance [brief | *group*]	Displays the VRRP Plus running status.
show vrrp balance interface *type number* **[brief]**	Displays the VRRP Plus running status o the specified interface.

Platform Description N/A.

4.7 vrrp weighting

Use this command to set the weight and threshold of the VRPP Plus backup group. Use the **no** form of this command to restore the two values to default.

vrrp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
no vrrp *group* **weighting**

Parameter Description

Parameter	Description
group	VRRP Plus backup group ID, in the range of 1 to 255.
maximum	Weight, 100 by default, in the range of 2 to 254.
lower	Weight lower, 1 by default, in the range of 1 to (maximum-1)
upper	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.

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.

```
Ruijie(config-if)# vrrp 1 ip 192.168.1.1
Ruijie(config-if)# vrrp 1 balance
Ruijie(config-if)# vrrp 1 weighting 50 lower 30 upper 50
```

Related Commands

Command	Description
vrrp *group* **balance**	Enables the VRRP Plus function.
show vrrp balance [brief | *group*]	Displays the VRRP Plus running status.
show vrrp balance interface *type number* **[brief]**	Displays the VRRP Plus running status of the specified interface.

Platform Description

N/A.

5 BFD Commands

5.1 bfd

Use this command to set the BFD session parameter in the interface configuration mode. 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
interval milliseconds	Interval of sending the BFD control messages to the BFD session neighbor. milliseconds: The range is from 50 to 10,000.
min_rx milliseconds	Expected interval of receiving the BFD control messages from the BFD session neighbor. milliseconds: The range is from 50 to 10,000.
multiplier multiplier-value	Count of BFD control message not received from the peer in the configured interval. multiplier-value: The range is from 3 to 50.

Defaults No BFD session parameter is configured by default. Those parameters must be configured before enabling the BFD session.

Command Mode Interface configuration mode.

Usage Guide Note that this command is not configurable on the L3 AP.
The express forwarding must be enabled before enabling BFD on the routers.

Configuration Examples The following example configures the BFD session parameter on routed port FastEthernet 0/2:

```
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 Description N/A

5.2 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
peer-ip ip-address	The peer IP address to be detected, which must be directly connected to the Layer3 interface.
source-ip ip-address	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.
process-pst	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 an Layer3 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 Description N/A

5.3 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 Description N/A

5.4 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 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 Layer 3 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.

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
bfd	Configures the BFD session parameter.
bfd slow-timer	Configures the slow-timer time.

Platform Description N/A

5.5 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

Parameter Description

Parameter	Description
milliseconds	BFD slow-timer time. The range is from 1,000 to 30,000. The unit is millisecond..

Defaults The default slow-timer is 3000 milliseconds.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the slow-timer to 14,000 milliseconds:

```
Ruijie(config)# bfd slow-timer 14000
```

Related Commands

Command	Description
bfd echo	Enables the BFD echo function

Platform Description N/A

5.6 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 up-dampening

Parameter Description

Parameter	Description
milliseconds	(Optional) Sets the BFD up-dampening time. The range is from 0 to 300,000. The unit is millisecond.

Defaults The default is 0, which means that the notification is sent to the related application once the session state is changed to UP.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the BFD up-dampening time to 60,000 milliseconds:

```
Ruijie(config)# bfd up-dampening 60000
```

Related Commands

Command	Description
bfd	Configures the BFD session parameter.

Platform Description N/A

5.7 show bfd neighbors

Use this command to display the BFD session parameters.

show bfd neighbors [**vrf** *vrf-name*] [**client** { **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** *ipv6-address*] [**details**]

Parameter Description

Parameter	Description
vrf *vrf-name*	(Optional) sets the neighbor VRF name.
client	(Optional) specifies the routing protocol.
bgp	Displays the BFD session configuration for BGP.
isis	Displays the BFD session configuration for ISIS.
ospf	Displays the BFD session configuration for OSPF.
ospfv3	Displays the BFD session configuration for OSPFv3.
rip	Displays the BFD session configuration for RIP.
vrrp	Displays the BFD session configuration for VRRP.
static-route	Displays the BFD session configuration for the static route.
pbr	Displays the BFD session configuration for PBR.
vrrp-balance	Displays the BFD session configuration for the VRPP.
bgp-lsp	Displays the BFD session configuration for the BGP-LSP.
ldp-lsp	Displays the BFD session configuration for the LDP-LSP.
backward-lsp-with-ip	Displays the BFD session configuration for the LSP backward IP co-operation.
static-lsp	Displays the BFD session configuration for the static LSP co-operation.
pst	Displays the BFD session configuration and the Layer3 interface status.
ipv4 *ip-address*	(Optional) Displays the session information of the specified IPv4 neighbor.
ipv6 *ipv6-address*	(Optional) Displays the session information of the specified IPv6 neighbor.
details	(Optional) Displays the configurations in detail.

Defaults N/A

Command Mode Privileged EXEC 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 Examples The following example displays the result of running the **show bfd neighbors** command:

```
Ruijie# show bfd neighbors
OurAddr       NeighAddr  LD/RD RH  Holdown(mult)  State     Int
```

```
172.16.11.1     172.16.11.2 1/2      1   532 (3 )  Up    Ge2/1
```

Field	Description
OurAddr	Local IP address.
NeighAddr	Neighbor IP address.
LD/RD	Local & Remote identifiers.
RH/RS	Whether the remote session responses the local session.
Holdown(mult)	Time of not receiving the hello packets for the local session and the times of the timeout detection.
State	The current session state.
Int	The interface number for the session.
Session state is UP and using echo function with 50 ms interval	Whether the session is in the echo mode and the echo interval (which is displayed only in the echo mode).
Local Diag	Session diagnostic information.
Demand mode	Whether the session poll mode is active or not.
Poll bit	Whether the session configuration has been modified or not.
MinTxInt	The minimum sending interval for the local session.
MinRxInt	The minimum receiving interval for the local session.
Multiplier	The timeout detection times for the local session.
Received MinRxInt	The minimum sending interval for the remote session.
Received Multiplier	The timeout detection times for the remote session.
Holdown (hits)	The session detection time and the times of the timeout detection.
Hello (hits)	The minimum interval of receiving the hello packets after the session negotiation.
Rx Count	The number of BFD packets received by the local session.
Rx Interval (ms) min/max/avg	The minimum, maximum and average intervals of receiving for the local session.
Tx Count	The number of BFD packets sent by the local session.
Tx Interval (ms) min/max/avg	The minimum, maximum and average intervals of sending for the local session.
Registered protocols	The registered protocol type of the session.
Uptime	The time of keeping the session UP.
Last packet	The last BFD packet information received by the local session.

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

6 IP Event Dampening Commands

6.1 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
half-life-period	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.
reuse-threshold	Configures the penalty threshold to unsuppress the interface. The range is from 1 to 20,000. The default value is 1,000.
suppress-threshold	Configures the penalty threshold to suppress the interface. The range is from 1 to 20,000. The default value is 2,000.
max-suppress	Configures the maximum suppress time. The range is from 1 to 255. The default value is 4 times of the *half-life-period.*
restart	Activates the restart penalty.
restart-*penalty*	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 transcieve 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.
Note: For routers, this function can be configured on the master interface only. This function takes effect for all sub-interfaces of the master interface with this command configured, but this command cannot be configured on the sub-interface directly. This command cannot be configured on the virtual template.

Configuration Examples The following example configures the IP event dampening function.

```
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
clear counters	Clears the interface counters.
show dampening interface	Displays the statistics of the dampening interface.
show interface dampening	Displays details of the dampening interface.

Platform Description N/A

6.2 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
dampening	Enables the IP event dampening function on the interface.
clear counters	Clears the interface counters.
show interface dampening	Displays details of IP event dampening configuration.

Platform Description N/A

6.3 show interface dampening

Use this command to display the details of IP event dampening configuration.

show interface [*interface-Id*] **dampening**

Parameter Description

Parameter	Description
interface-id	Interface name

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 Examples The following example shows the details of IP event dampening configuration.

```
Ruijie# show interface 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
dampening	Enables the IP event dampening function.
clear counters	Clears the interface counters.
show dampening interface	Displays statistics of the dampening interface.

Platform Description N/A

7 VSU Commands

7.1 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 Description

Parameter	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)# dad relay enable
```

The following example disables the AP-based DAD relay function.

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# no dad relay enable
```

Related Commands

Command	Description
dual-active detection	Configures DAD.
dual-active pair interface	Configures a pair of Bidirectional Forwarding Detection (BFD)-based DAD interfaces.
dual-active exclude interface	Configures an exclude interface of DAD.
show switch virtual dual-active	Displays the configuration and status of DAD.

Platform Description N/A

7.2 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 Description

Parameter	Description
interface-name	Interface name

Defaults N/A.

Command Mode config-vs-domain mode.

Usage Guide The BFD port must be a routing port on the peer end.

Configuration Examples The following examples configures interface Gi 1/1/1 as a BFD port.

```
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 Commands

Command	Description
N/A	N/A

Platform Description N/A

7.3 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 Description

Parameter	Description
bfd	BFD-based DAD.
aggregateport	AP-based DAD.

Defaults This function is disabled by default.

Command Mode config-vs-domain 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
dual-active pair interface	Configures a DAD interface.
dual-active exclude interface	Configures an exclude interface of DAD.
show switch virtual dual-active	Displays the configuration and status of DAD.

Platform Description N/A

7.4 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
interface-name	Interface type and interface number.

Defaults N/A

Command Mode config-vs-domain mode.

Usage Guide Configure this command only in VSU mode.

After the VSU works in dual-active chassis mode, to remotely log in to the management device from an interface, you can run the **dual-active exclude interface** command to set this interface to an interface that is not disabled in recovery mode.

An exclude interface must be a routing interface instead of a virtual switch link (VSL) interface.

Multiple exclude interfaces are supported.

Configuration Examples The following example configures interface Gi 1/1/3 as an exclude interface of DAD.

```
Ruijie(config)# interface GigabitEthernet 1/1/3
Ruijie(config-if)# no switchport
Ruijie(config-if)# ip address 3.1.1.1 255.255.255.0
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active exclude interface GigabitEthernet 1/1/3
```

Related Commands

Command	Description
dual-active detection	Configures DAD.
dual-active pair interface	Configures a DAD interface.
show switch virtual dual-active	Displays the configuration and status of DAD.

Platform Description N/A

7.5 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
interface-name	Interface type and interface number. An AP-based DAD interface must be specified.

Defaults N/A

Command Mode config-vs-domain 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 Examples The following example configures AP 1 as the AP-based detection interface.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active interface aggregateport 1
```

Related Commands

Command	Description
dual-active detection	Configures BFD-/AP-based DAD.
show switch virtual dual-active	Displays the configuration and status of DAD.

Platform Description N/A

7.6 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 *interfacename* [**copper | fiber**]

no port-member interface *interfacename*

Parameter Description

Parameter	Description
interfacename	Interface name, for example, GigabitEthernet 0/1 and GigabitEthernet 0/3.
copper	Copper port
fiber	Fiber port

Defaults N/A

Command Mode config-vsl-port mode.

Usage Guide Configure this command in VSU mode or in standalone mode.

The command configured in standalone mode takes effect only in VSU mode.

The command configured in VSU mode takes effect immediately.

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 1/0/1
Ruijie(config-vsl- port)# no port-member interface GigabitEthernet 1/0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.7 session

Use this command to perform redirection to a host or a device console.

session { **device** *switch_id* | **master** }

Parameter Description

Parameter	Description
device	Redirects to the member device console.
switch_id	Member device number, in the range from 1 to 8.
master	Redirects to the host console.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command takes effect in VSU mode.

Configuration Examples The following example redirects the serial port console of standby device 2 to the master device console.

```
Ruijie-STANDBY#session master
Ruijie#exit
Ruijie-STANDBY#
```

The following example redirects the master device console to the console of standby device 2 and exits.

```
Ruijie#session device 2
Ruijie-STANDBY#exit
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.8 show switch id

Use this command to display the switch ID of the device.

show switch id

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 switch ID of the device in the standalone mode.

```
Ruijie#show switch id
Switch ID is 2
```

The following example displays the switch ID of the device in the VSU device.

```
Ruijie#show switch id
Switch ID is 1
```

Related Commands

Command	Description
show switch virtual	Displays the domain ID as well as the ID and role of each chassis.

Platform Description N/A

7.9 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

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
switch	Modifies the device ID in standalone mode.
switch priority	Configures the device priority.
switch renumber	Modifies the device ID in VSU mode.
switch domain	Modifies the domain ID of a device in VSU mode.
switch virtual domain	Modifies the domain ID of a device in standalone mode.

Platform Description N/A

7.10 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 Examples The following example displays the load balance configuration of the device in VSU mode.

```
Ruijie#show switch virtual balance
Aggregate port LFF: enable
```

Related Commands

Command	Description
show switch virtual	Display the domain ID as well as the ID and role of the device.

Platform Description N/A

7.11 show switch virtual config

Use this command to display the VSU configuration of the device in standalone or VSU mode.

show switch virtual config

Parameter Description

Parameter	Description
switch_id	Displays the VSU configuration of the specified device.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the VSU configuration of the device in standalone mode.

```
Ruijie#show switch virtual config
mac: 00d0.f810.3323
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
!
vsl-port 1
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
!
vsl-port 1
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 1
port-member interface GigabitEthernet Ethernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
```

Related Commands

Command	Description
show switch virtual	Displays the domain ID as well as the ID and role of each chassis.

Platform Description N/A

7.12 show switch virtual dual-active

Use this command to display the configuration of DAD.

show switch virtual dual-active { **bfd | aggregateport | summary** }

Parameter Description

Parameter	Description
bfd	Configuration of BFD-based DAD.
aggregateport	Configuration of AP-based DAD.
summary	Configuration and status of DAD.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the configuration and status of DAD.

```
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 1/1/3
GigabitEthernet 1/1/4In 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 pairs configured:
Pair interface GigabitEthernet 1/0/1 and interface GigabitEthernet 2/0/1:
UP
Pair interface GigabitEthernet 1/0/2 and interface 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
dual-active detection	Enables DAD.
dual-active pair interface	Configures a DAD interface.
dual-active exclude interface	Configures an exclude interface.

Platform Description N/A

7.13 show switch virtual link

Use this command to display the status of a virtual switch link (VSL).

show switch virtual link [**port**]

Parameter Description

Parameter	Description
port	Displays the port status of a VSL.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays VSL link information.

```
Ruijie# show switch virtual link
VSL-AP   State   Peer-VSL   Rx         Tx         Uptime
------- ------- ---------- --------- ----------- -------------
1/1     UP      2/1        657976     694603     0d,1h,42m
2/1     UP      1/1        694856     658174     0d,1h,42m
```

The values of **VSL Status** are **DOWN** and **UP**.

The following example displays VSL port information.

```
Ruijie# show switch virtual link port
VSL-AP-1/1:Port           State   Peer-port                Rx      Tx
Uptime
------------------------- ------- ------------------------- --------
-------- ----------
TenGigabitEthernet 1/4/1   DOWN    -                        0       0
-
TenGigabitEthernet 1/4/3   DOWN    -                        27      0
-
TenGigabitEthernet 1/8/1   DOWN    -                        112494   186930
-
TenGigabitEthernet 1/8/2   OK      TenGigabitEthernet 2/8/1   544825
507008   0d,1h,42m
VSL-AP-2/1:
Port                    State   Peer-port                Rx      Tx
Uptime
------------------------------------------------------------ --------
-------- ----------
TenGigabitEthernet 2/1/1   DOWN    -                        0       0
-
TenGigabitEthernet 2/1/2   DOWN    -                        0       0
-
TenGigabitEthernet 2/1/4   DOWN    -                        11      0
-
TenGigabitEthernet 2/8/1   OK      TenGigabitEthernet 1/8/2   506915
544730   0d,1h,42m
TenGigabitEthernet 2/8/2   DOWN    -                        186930   112495
-
```

A VSL interface can be in the UP, DOWN, or OK state.

Related Commands

Command	Description
show switch virtual	Displays information about the VSU system.
show switch virtual role	Displays the ID, role, and priority of each device.

Platform Description N/A

7.14 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
switch priority	Configures the priority of a device in the VSU system.
switch virtual domain	Modifies the domain ID of a device in standalone mode.
show switch virtual link	Displays VSL information.

Platform Description N/A

7.15 show switch virtual topology

Use this command to display the VSU topology connection status.

show switch virtual topology

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 topology status.

```
Ruijie# show switch virtual topology
Introduction: '[num]' means switch num, '(num/num)' means vsl-aggregateport
num.

Ring Topology:
[1](1/2)---(2/1)[2](2/2)---(1/1)[1]

Switch[1]: ACTIVE, MAC: 00d0.f822.33d6, Description: Switch1
Switch[2]: STANDBY, MAC: 1234.5678.9003, Description: Switch2
```

Field	Description
Ring Topology	Topology type.
Switch[-]	Device description.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.16 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		
	switch_id	ID of a device in the VSU system. The range is from 1 to 4 for a chassis device and from 1 to12 for a box device.

Defaults The default is 1.

Command Mode config-vs-domain 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 both 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
```

Related Commands

Command	Description
switch virtual domain	Modifies the domain ID of a device in standalone mode.
switch priority	Configures the priority of a device in the VSU system.
show switch virtual	Displays the domain ID as well as the ID and role of each chassis.

Platform Description N/A

7.17 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 Description

Parameter	Description
virtual	VSU mode.
standalone	Standalone mode.
switch_id	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 Examples

The following example demonstrates how to set the domain ID to **1**, device ID to **1**, as well as device priority to **200**, and how to convert the device mode from the standalone mode into the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# end
Ruijie# switch convert mode virtual
```

The following example demonstrates how to first switch 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
switch	Modify the device ID in standalone mode.
switch virtual domain	Modify the domain ID of a device in standalone mode.
switch priority	Configure the priority of a device in the VSU system.
show switch virtual	Display the domain ID as well as the ID and role of each chassis.

Platform Description

V

7.18 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 Description

Parameter	Description
error_num	Limits the number of error frames increasing from that in the last detection. If the increased number is greater than *error_num*, it is taken as an error.
time_num	When the error count exceeds the *time_num*, 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 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

7.19 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 Description

Parameter	Description
switch_id	Device ID.
dev_name	Device description, no greater than 12 characters.

Defaults N/A

Command Mode config-vs-domain mode

Usage Guide This command is configured on a device in whether standalone or VSU mode and takes effect

immediately after configuration,

Configuration Examples The following example configures the description for a VSU switch.

```
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

7.20 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
switch_id	ID of the running device in VSU mode. The range is from 1 to 4 for a chassis device and from 1 to 12 for a box device.
new_domain_id	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 mode.

Usage Guide Use this command only in VSU mode. In addition, the setting can take effect only after the device is restarted.

Configuration Examples The following example sets the domain ID of device 1 to **10** in VSU mode.

```
Ruijie(config-vs-domain)# switch 1 domian 10
Changing the domain ID may cause VSU establishment failure after the next
startup. Are you sure to continue? [N/Y]y
```

The following example sets the domain ID of device 2 to the default value in VSU mode.

```
Ruijie(config-vs-domain)# no switch 2 domain
Changing the domain ID may cause VSU establishment failure after the next
startup. Are you sure to continue? [N/Y]y
```

Related Commands

Command	Description
switch virtual domain	Modifies the domain ID in standalone mode.
show switch virtual	Displays the domain ID as well as the ID and role of each chassis.

Platform Description N/A

7.21 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**

Parameter Description

Parameter	Description
switch_id	ID of a device in the VSU system. The range is from 1 to 4 for a chassis device and from 1 to 12 for a box device.
priority_num	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 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.

This command is not used to modify the value of **switch_id**. In standalone mode, if **switch_id** is set to **1**, running the **switch 2 priority 200** command does not take effect. In this case, set **switch_id** to **2** and then run the **switch 2 priority 200** command.

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
```

```
Changing the priority of the switch may cause the master switch and the slave switch different from the current ones after the next startup. Are you sure to continue? [N/Y]y
Ruijie(config-vs-domain)# no switch 2 priority
Changing the priority of the switch may cause the master switch and the slave switch different from the current ones after the next startup. Are you sure to continue? [N/Y]y
Ruijie(config-vs-domain)# exit
```

Related Commands

Command	Description
switch	Modifies the device ID in standalone mode.
show switch virtual	Displays the domain ID as well as the ID and role of each chassis.

Platform Description N/A

7.22 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*

Parameter Description

Parameter	Description
switch_id	ID of the running device in VSU mode, which can be **1** (by default) or **2**. The range is from 1 to 4 for a chassis device and from 1 to 12 for a box device.
new_switch_id	New device ID. The range is from 1 to 4 for a chassis device and from 1 to 12 for a box device.

Defaults N/A

Command Mode config-vs-domain mode.

Usage Guide This command is configured in VSU mode. In addition and takes affect after device restart.

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
Renumbering the switch ID may result in configuration change or loss. Are you sure to continue? [N/Y]y
```

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
Renumbering the switch ID may result in configuration change or loss. Are you sure to continue? [N/Y]y
```

Related Commands

Command	Description
switch	Modifies the device ID in standalone mode.
show switch virtual	Displays the domain ID as well as the ID and role of each chassis.

Platform Description N/A

7.23 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 Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default..

Command Mode config-vs-domain 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
show switch virtual balance	Displays the current traffic balancing mode.

Platform Description N/A

7.24 switch virtual domain

Use this command to modify the domain ID of a device in standalone mode. Use the **no** form of this command to restore the default setting.

switch virtual domain *domain_id*

no switch virtual domain

Parameter Description

Parameter	Description
domain_id	Domain ID of the VSU, in the range from 1 to 255.

Defaults The default is 100.

Command Mode config-vs-domain 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).

Use this command in standalone mode.

In standalone mode, this command can be used to modify the value of **domain_id** and enter the config_vs_domain mode.

In VSU mode, this command can be only used to enter the **config_vs_domain** mode. In VSU mode, you can use the **switch domain** command to modify the value of **domain_id**.

Configuration Examples The following example sets the domain ID of the VSU to **1** in standalone mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)#
```

The following example enters the domain configuration mode in VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)#
```

Related Commands

Command	Description
show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
switch domain	Modifies the domain ID in VSU mode.

Platform Description N/A

7.25 switch virtual ecmp lff enable

Use this command to enable the locally-preferred forwarding function on the ECMP interface in VSU mode and disable cross-chassis ECMP traffic balancing. Use the **no** form of this command to restore the default setting.

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 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
	show switch virtual balance	Displays the current load balance mode.

Platform Description N/A

7.26 vsl-port

Use this command to enter VSL-PORT mode

vsl-port

Parameter Description	Parameter	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 Examples The following example enters VSL-AP configuration mode on a device in standalone mode.

```
Ruijie(config)# vsl-port
Ruijie(config-vsl-port)#
```

The following example enters VSL-APPORT 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

8 VSD Commands

8.1 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
interface *int_index*	Labels of physical ports

Defaults All physical ports belong to the default VSD, also known as VSD0.

Command Mode VSD configuration mode

Level 14

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 Examples The following example allocates physical ports to a non-default VSD (named admin).

```
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
```

Verification Use the **show vsd membership** command to display all physical port resources in a VSD.

Prompt Messages If your input port No. does not include No. of all ports in a group, the port No. will automatically include the rest of ports in the group.

```
Interface-group[2/2/1 ~ 2/2/44] and their config will be removed from vsd[0].
```

You need to make sure whether to continue allocating ports with VSL port to get rid of VSU topological devision.

```
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]
```

The allocated port is already allocated for another VSD.

```
This interface is already allocated for another vsd.
```

The allocated port is already allocated for this VSD.

```
This interface is already allocated for this vsd.
```

Common Errors

1. You reclaim a port that does not belong to a non-default VSD.
2. You allocate a port for another VSD which is allocated to a non-default VSD without reclaiming it.

Platforms N/A

8.2 allocate slot

Use this command to allocate multi-service card resources to a VSD.

allocate slot *slot_id*

Use the **no** form of this command to reclaim multi-service card resources allocated to a non-default VSD.

no allocate slot *slot_id*

Parameter Description

Parameter	Description
slot *slot_id*	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

Level 14

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 Examples The following example allocates multi-service cards to a non-default VSD (named admin).

```
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)#
```

Verification Use the **show vsd membership** command to display the multi-service card resources in a VSD.

Prompt Messages You need to make sure whether to allocate the multi-service card to another VSD which may cause same service in source VSD to stop.

```
Allocating slot 1/2 may cause some service in source vsd to stop. Are you sure
to continue (y/n)? [no]
```

The multi-service card is already allocated to another VSD.

```
This slot is already allocated for another vsd.
```

The multi-service card is already allocated to this VSD.

```
This slot is already allocated for this vsd.
```

Common Errors 1. You reclaim a port that does not belong to a non-default VSD.
2. You allocate a port to another VSD which is already allocated to the non-default VSD without reclaiming it.

Platforms N/A

8.3 show vsd

Use this command to display the VSD information.

show vsd { **current-vsd | { { membership | detail | all** } [*vsd_name*] } }

Parameter Description

Parameter	Description
current-vsd	Name and ID of the current VSD
membership	Displays physical port resources and multi-service resources in a VSD.
detail	Displays detailed information about a VSD including its ID, name and MAC address.
all	Displays full information about a VSD including its ID, name and MAC address, physical port resources and multi-service resources.
vsd_name	Specifies a VSD. It refers to a VSDO, by default.

Command Mode Privileged EXEC mode/ Global configuration mode

Level 14

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 Examples The following example displays the ID and name of the current VSD.

```
Ruijie# sho vsd current-vsd
Current vsd is 1 – Ruijie
Ruijie #
```

Field Description

Field	Description
Current vsd is 0	ID of the current VSD
Ruijie	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:  Ruijie
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:  Ruijie
mac address:  00d0.f822.33c2
```

```
vsd_id:  1
vsd_name:  production
mac address:  00d0.f822.33c3
```

Field Description

Field	Description
vsd_id	ID of a VSD
vsd_name	Name of a VSD
mac address	MAC Address of a VSD

The following example displays the whole information about a VSD.

```
Ruijie#show vsd all
vsd_id:  0
vsd_name:  Ruijie
vsd mac address:  00d0.f822.33c0
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
interface:
       NA
slot:
       NA
```

Field Description

Field	Description
vsd_id	ID of a VSD
vsd_name	Name of a VSD
vsd mac address	MAC address of a VSD
interface	Physical port resources
slot	Multi-service card resources

Prompt Messages N/A

Platforms N/A

8.4 switchback

Use this command to switch back from the non-default VSD to the default VSD.

switchback

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Level 14

Usage Guide 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).

Configuration Examples The following example switches back from a non-default VSD (named admin) to the default VSD.

```
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#
```

Prompt Messages N/A

Platforms N/A

8.5 switchto vsd

Use this command to log in from the default VSD to a non-default VSD.

switchto vsd *vsd_name*

Parameter

Parameter	Description

Description

vsd *vsd_name*	Name of a non-default VSD

Command Mode Privileged EXEC mode

Level 14

Usage Guide This command is used to log in from the default VSD to a non-default VSD.

Configuration Examples The following example logs in from the default VSD to a non-default VSD (named admin).

```
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#
```

Prompt Messages The VSD information will be displayed after you log in to a non-default VSD.

```
Ruijie General Operating System Software
Copyright (c) 1998-2013s by Ruijie Networks.
All Rights Reserved.
Neither Decompiling Nor Reverse Engineering Shall Be Allowed.
```

Platforms N/A

8.6 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
vsd *vsd_name*	Name of a non-default VSD
id *vsd_number*	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

Level 14

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).

```
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)#
```

Verification Use the **show vsd** command to display all the non-default VSDs created currently.

Prompt Messages You create a non-default VSD without license.

```
Enable LIC-N18000-VSD failed:  the service haven't been licensed before.
```

```
Log on website "http://192.168.5.227:8080/login.jsf" to get the corresponding
license file, then try "license install" it under global configuration.
```

Prompt messages appear during your creating VSD for several seconds.

```
Note:  Creating VSD, one moment please ...
```

The VSD configuration will be removed as VSD is deleted. You need to make sure whether to allocate ports which may cause VSU topological division because of the VSL port on this card.

```
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 ...
```

Common Errors You create a non-default VSD without license.

Platforms N/A

9 NLB Group Commands

9.1 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
group-number	Cluster group number
vrf-name	VRF name
nlb-address	NLB address
reflector-port *interface-name*	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.
destination-port *interface-name*	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 L2AP can be both configured as the cluster connecting port. However, only the Switch Port can be set as the reflector 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.

Use the **show nlb-group** command to display the cluster configuration.

1. After a port has been configured as a reflector port, other configurations are not allowed for

this port. .

2. One port cannot be both the reflector port and connecting port. .

3. After configuring the cluster attributes, the cluster service is enabled only on the connecting port with cluster configured. .

4. If no cluster attribute is configured, the cluster service is not enabled. .

5. No VRF keyword means the global VRF takes effect. .

6. Up to 5 cluster groups can be configured on each switch and up to16 connecting ports are configurable on per cluster group.

Configuration Examples The following example creates a cluster group and configures the cluster attributes and the cluster connecting port.

```
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(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(config)# no nlb-group 1 destination-port gigabitethernet 0/2, 0/3
```

Related Commands

Command	Description
show nlb-group	Displays the cluster configuration.

Platform Description N/A

9.2 show nlb-group

Use this command to display the cluster configuration.

show nlb-group [*group_number*].

Parameter Description

Parameter	Description
group-number	Cluster group number

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode

Usage Guide N/A

Configuration Examples The following example displays the cluster configuration.

```
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
nlb-group	Creates a cluster group and specify the cluster attributes and the port connecting the cluster with device.

Platform Description N/A

Network Management & Monitoring Configuration 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 | process-mib-time**]

Parameter Description

Parameter	Description
mib	Displays the SNMP MIBs supported.
user	Displays the SNMP user information.
view	Displays the SNMP view information.
group	Displays the SNMP user group information.
host	Displays the explicit host configuration.
process-mib-time	Displays the MIB node requiring the longest processing time.

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The example below displays the SNMP configuration:

```
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
```

Related Commands

Command	Description
snmp-server chassis-id	Specifies the SNMP system sequence number.

Platform Description N/A

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 Description

Parameter	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 Examples The following example disables the interface to send link traps.

```
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 Description N/A

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 Description

Parameter	Description
text	SNMP chassis ID: numerals or characters.

Defaults The default is 60FF60.

Command mode Global configuration 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 Examples The following example specifies the SNMP chassis ID as 123456:

```
Ruijie(config)# snmp-server chassis-id 123456
```

Related Commands

Command	Description
show snmp	Displays the SNMP configuration.

Platform Description N/A

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.
string	Community string, which is the communication password between the NMS and the SNMP agent
view-name	View name
ro	Indicates that the NMS can only read the variables of the MIB.
rw	Indicates that the NMS can read and write the variables of the MIB.
aclnum	Access list number (1 to 199, and 1300 to 2699), which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Access list name, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6-aclname	IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
ipaddr	Specifies the IP address of the NMS to access the MIB.

Defaults All communities are read only by default.

Command mode Global configuration 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
access-list	Defines an access list.

Platform Description N/A

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
text	Defines a system contact string.

Defaults No system contact string is set by default.

Command mode Global configuration 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
show snmp-server	Displays the SNMP configuration.
no snmp-server	Disables the SNMP agent function.

Platform Description N/A

1.7 snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap massage to NMS. Use the **no** form of this command to disable the SNMP agent to send the SNMP trap massage to NMS.

snmp-server enable traps [*notification-type*]

no snmp-server enable traps

Parameter Description

Parameter	Description
notification-type	Specifies the type of trap messages. snmp: SNMP trap message bgp: BGP trap message. bridge: Bridge trap message. isis: ISIS trap message. mac-notification: MAC trap message. ospf: OSPF trap message. urpf: uRPF trap message. vrrp: VRRP trap message. 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 Examples The following example enables the SNMP agent to send the SNMP trap message.

```
Ruijie(config)# snmp-server enable traps snmp
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host to send the SNMP trap message.

Platform Description N/A

1.8 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** } }

Parameter Description

Parameter	Description
v1 | **v2c** | **v3**	Specifies the SNMP version
auth	Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only.
noauth	Specifies no authentication a packet. This applies to SNMPv3 only.
priv	Specifies authentication of a packet with encryption. This applies to SNMPv3 only.
readview	Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.
writeview	Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
aclnum	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6_aclname	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 Examples The following example configures a new SNMP group.

```
Ruijie(config)# snmp-server group mib2user v3 priv read mib2
```

Related Commands

Command	Description
show snmp group	Displays the SNMP group configuration.

Platform Description N/A

1.9 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*] [*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*]

Parameter Description

Parameter	Description
oob	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.
host-addr	SNMP host address
ipv6-addr	SNMP host address(ipv6)
vrfname	Set the name of vrf forwarding table
trap | informs	Enables the host to send the SNMP notification as traps or informs.
version	SNMP version: V1, V2C or V3
auth | **noauth** | **priv**	Security level of SNMPv3 users
community-string	Community string or username (SNMPv3 version)
port-num	Port of the SNMP host
notification-type	The type of the SNMP trap message, such as **snmp**. 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.

Configuration Examples The following example specifies an SNMP host to receive the SNMP event trap:

```
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

Related Commands

Command	Description

snmp-server enable traps	Enables the SNMP agent to send the SNMP trap message.

Platform Description N/A

1.10 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
text	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 Examples The following example sets the system location information:

```
Ruijie(config)# snmp-server location start-technology-city 4F of A Buliding
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact information.

Platform Description N/A

1.11 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

get-operation	Logging function for the GET and GET-NEXT operations.
set-operation	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 Examples The following example enables the logging function for the GET and SET operations:

```
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 Description N/A

1.12 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
text	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 Examples The following example configures the network element coding text to FZ_CDMA_MSC1.

```
Ruijie(config)# snmp-server net-id FZ_CDMA_MSC1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.13 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
byte-count	Packet size. The range is from 484 to 17,876 bytes

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 Examples N/A

Related Commands

Command	Description
snmp-server queue-length	Specifies the length of the message queue for each SNMP trap host.

Platform Description N/A

1.14 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
length	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.

The maximum speed to send messages is 4 messages per second.

Configuration Examples The following example specifies the length of message queue as 4.

```
Ruijie(config)# snmp-server queue-length 4
```

Related Commands

Command	Description
snmp-server packetsize	Specifies the largest size of the SNMP packet.

Platform Description N/A

1.15 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 Examples The following example enables the SNMP message reload function:

```
Ruijie(config)# snmp-server system-shutdown
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.16 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 Examples The following example configures the SNMP trap format with the private field.

```
Ruijie(config)# snmp-server trap-format private
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.17 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
interface	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
snmp-server enable traps	Enables t the SNMP agent to send the SNMP trap massage to NMS.
snmp-server host	Specifies the NMS host to send the SNMP trap message.

Platform Description N/A

1.18 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
seconds	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
snmp-server queue-length	Specifies the length of message queue for the SNMP trap host.
snmp-server host	Specifies the NMS host to send the SNMP trap message.
snmp-server trap-source	Specifies the source address of the SNMP trap message.

Platform Description N/A

1.19 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
port-number	Specifies a port to receive the SNMP packets.

Defaults The default is 161.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies port 15000 to receive the SNMP packets.

```
Ruijie(config)# snmp-server udp-port 15000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.20 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
username	Name of the user on the host that connects to the agent.
groupname	Name of the group to which the user belongs.
v1 | v2c | v3	Specifies the SNMP version. But only SNMPv3 supports the following security parameters.
encrypted	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.
auth	Specifies which authentication level should be used.
auth-password	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
priv	Encryption mode. des56 refers to 56-bit DES encryption protocol. *priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
md5	Enables the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
aclnumber	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6_aclname	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
show snmp user	Displays the SNMP user configuration.

Platform Description N/A

1.21 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 Description

Parameter	Description
view-name	View name
oid-tree	Specifies the MIB object to associate with the view.
include	Includes the sub trees of the MIB object in the view.
exclude	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 Examples The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

```
Ruijie(config)# snmp-server view mib2 1.3.6.1 include
```

Related Commands

Command	Description
show snmp view	Displays the SNMP view configuration.

Platform Description N/A

1.22 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 [**retries** | **timeout**]

Parameter Description

Parameter	Description
retry-num	Specifies the resend times for inform requests, ranging from 0 to 255.
time	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

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 description

Parameter	Description
number	Alarm number. The value ranges from 1-65,535.
variable	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).
interval	Sampling interval. The valye ranges from 1 to 2,147,483,647 in the unit of second.
absolute	Absolute sampling. In this mode, when the sampling time arrives, the system directly invokes the variable value.
delta	Delta sampling. In this mode, when the sampling time arrives, the system invokes the delta value of the variable within the sampling interval.
rising-threshold *value*	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.
event-number	The event number ranges from 1 to 65,535.
falling-threshold *value*	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
owner *ownername*	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
rmon event *number* [**log**] [**trap** *community*] **description** *string* [**owner** *owner-string*]	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
index	Index of a history entry. The value ranges from 1 to 65,535.
owner *ownername*	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.
buckets *bucket-number*	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.
interval *seconds*	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.

Examples The example below enables log statistics 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-GigabitEthernet0/1)#rmon history 1 owner UserA buckets 5
interval 60
```

Related commands

Command	Description
rmon collection stats *index* [owner *owner-name*]	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
index	Index of the statistic table. The value ranges from 1 to 65,535.
owner *ownername*	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.

Examples The example below enables monitoring the statistics of 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-GigabitEthernet0/1)# rmon stats 1 owner UserA
```

Related commands

Command	Description
rmon collection history *index* [**owner** *owner-name*] [**buckets** *bucket-number*] [**interval** *seconds*]	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
number	Event number. The value ranges from 1 to 65,535.
log	(Optional) Log event. When a log event is triggered, the system records a log.
trap *community*	(Optional) Trap event. When a trap event is triggered, the system sends trap with the group named “community”.
description *description-string*	(Optional) Description of the event. The value is a character string consisting of 1 to 127 characters.

owner *owner-name*	(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
```

Related commands

Command	Description
rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Adds an alarm entry.

2.5 show rmon

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

Use this command to display the RMON alarm table.

show rmon alarm

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples The example below displays the RMON alarm table.

```
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
rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	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.

Examples

The example below displays the event configuration.

```
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
rmon event *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	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.

Examples

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

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
rmon collection history *index* [owner *ownername*] **[buckets** *bucket-number*] **[interval** *seconds*]	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 N/A.

Examples

The example below displays the RMON statistics.

```
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
rmon collection stats *index* [**owner** *owner-string*]	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 Examples The following example disables NTP.

```
Ruijie(config)#no ntp
```

Related Commands

Command	Description
ntp server	Specifies an NTP server.

Platform Description N/A

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
peer	Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list.

serve	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.
serve-only	Allows the device to receive only time requests from the servers specified in the access list.
query-only	Allows the device to receive only NTP control queries from servers specified in the access list.
access-list-number	Access control list number, ranging from 1 to 99 and 1300 to 1999.
access-list-name	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
ip access-list	Creates an IP access control list.

Platform Description N/A

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 wooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp authenticate
```

Related Commands

Command	Description
ntp authentication-key	Sets the global authentication key.
ntp trusted-key	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
key-id	Key ID, ranging from 1 to 4294967295.
key-string	Key string

enc-type	(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 Examples The following example configures an NTP authentication key.

```
Ruijie(config)ntp authentication-key 6 md5 wooooop
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp trusted-key	Configures an NTP trusted key.
ntp server	Specifies an NTP server.

Platform Description N/A

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 Examples The following example disables the device to receive the NTP packets.

```
Ruijie(config-if)# no ntp disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
stratum	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 t 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 Examples The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12:

```
Ruijie(config)# ntp master 12
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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**]

no ntp server *ip-addr*

Parameter Description

Parameter	Description
oob	(Optional) Accesses the NTP server from the MGMT interface. By default, this option is disabled.
vrf *vrf-name*	Specifies the virtual routing and forwarding (VRF) name. By default, this parameter is disabled.
ip-addr	Sets the IP address of the NTP server. The address can be in IPv4 or IPv6 format.
domain	Sets the domain name of the NTP server, supporting IPv4 and IPv6.
version	(Optional) Specifies the NTP version (1-3). The default is NTPv3.
if-name	(Optional) Specifies the source interface from which the NTP message is sent (L3 interface).
keyid	(Optional) Specifies the encryption key adopted when communication with the corresponding server. The key ID range is from 1 to 4,294,967,295.
prefer	(Optional) Specifies the given NTP server as the preferred one.

Defaults No NTP server is configured by default.

Command mode Global configuration 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 Examples The following example configures an NTP server.
For IPv4: `Ruijie(config)# ntp server 192.168.210.222`
For IPv6: `Ruijie(config)# ntp server 10::2`

Related Commands

Command	Description
no ntp	Disables NTP.

Platform Description N/A

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
key-id	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 Examples The following example configures an authentication key and sets it as a trusted key.

```
Ruijie(config)#ntp authentication-key 6 md5 wooooop
Ruijie(config)#ntp trusted-key 6
```

```
Ruijie(config)#ntp server 192.168.210.222 key 6
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Configures an NTP authentication key.
ntp server	Configures an NTP server.

Platform Description N/A

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 Examples The following example configures the NTP update calendar periodically.

```
Ruijie(config)# ntp update-calendar
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 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 Examples The following example displays the NTP configuration.

```
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 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 Description

Parameter	Description
N/A	N/A

Defaults SNTP is disabled by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example enables SNTP.

```
Ruijie(config)# sntp enable
```

Related Commands

Command	Description
show sntp	Displays the SNTP configuration.

Platform Description N/A

4.2 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

Parameter Description

Parameter	Description
seconds	Synchronization interval. The unit is second, and the range is from 60 to 65,535.

Defaults The default synchronization interval is 1,800 seconds.

Command mode Global configuration mode.

Usage Guide To make the synchronization interval configuration effective, run the **sntp enable** command.

Configuration Examples The following example configures the synchronization interval to 3,600 seconds.

```
Ruijie(config)# sntp interval 3600
```

Related Commands

Command	Description
sntp enable	Enables SNTP.
show sntp	Displays the SNTP configuration.

Platform Description N/A

4.3 sntp server

Use this command to specify an SNTP server. Use the **no** form of this command to remove the SNTP/NTP server.

sntp server [**oob**] *ip-address*

no sntp server

Parameter Description

Parameter	Description
ip-address	IP address of the NTP/SNTP server.
oob	MGMT interface

Defaults No NTP/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 Examples The following example specifies an NTP server in Internet.

```
Ruijie(config)# sntp server 192.168.4.12
```

Related Commands

Command	Description
show sntp	Displays the SNTP configuration.
sntp enable	Enables SNTP.

Platform Description N/A

4.4 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 Examples The following example displays the SNTP configuration.

```
Ruijie# show  sntp
SNTP state          : Enable
SNTP server         : 192.168.4.12
SNTP sync interval   : 60
Time zone            : +8
```

Related Commands

Command	Description
sntp enable	Enables SNTP.

Platform Description N/A

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 disable 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. It is recommended the MAC loopback feature be enabled on the down interfaces.

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 Description N/A

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**] [**acl** *acl-name*]

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* [**encapsulation replicate** | **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* [**reflector-port**] **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 remote 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
session_number	SPAN session number
interface-id	Interface name
acl *acl-name*	Access list name
remote-vlan-id	Remote VLAN ID
vlan-id	VLAN ID (remote VLAN excluded)
vlan-id-list	VLAN list (remote VLAN excluded)
rx	Monitors the only received traffic.
tx	Monitors the only transmitted traffic.
both	Monitors both received and transmitted traffic. This is the default.
encapsulation	Specifies that the destination port replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).
switch	Enable switching on the mirroring destination port. It is disabled by default. Enables switching on the destination port. Switching function is disabled by default.
reflector-port	This parameter is required for one-to-many remote SPAN.

Defaults N/A

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** and **encapsulation replicate** features are disabled on the destination port.

Configuration Examples

The following example configures the source port and destination port of the SPAN session.

```
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 reflector port of the remote SPAN session.

```
Ruijie(config)# monitor session 4 destination remote vlan 10 reflector-port
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 Examples The following example configures a remote SPAN VLAN.

```
Ruijie(config)# vlan 100
Ruijie(config-vlan)# remote-span
```

Related Commands

Command	Description
show vlan	Displays VLAN configuration.

Platform Description N/A

5.4 show monitor

Use this command to display the SPAN configurations.

show monitor [**session** *session_number*]

Parameter Description

Parameter	Description
session_number	Displays the specified SPAN session.

Defaults N/A

Command mode Privileged EXEC mode, global configuration mode and interface configuration mode

Usage Guide N/A

Configuration Examples This following example displays all SPAN sessions.

```
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* }

Use this command to delete the address of the sFlow Agent.
no sflow agent address

Use this command to restore the default setting.
default sflow agent address

Parameter Description

Parameter	Description
ip-address	sFlow Agent IPv4 address.
ipv6 *ipv6-address*	sFlow Agent 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 filed 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 Messages Prompt an error message when the address is invalid.

```
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]]**

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]]**

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]]**

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.
ip-address	sFlow Collector IPv4 address
ipv6 *ipv6-address*	sFlow Collector IPv6 address
udp-port	sFlow Collector listening port number
vrf *vrf-name*	VRF instance name. It is not configured by default.
oob	The sampled traffics are output through the management interface. By default, this parameter is not configured.

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
collector-id	sFlow Collector ID. The range is from 1 to 2.
max-datagram-size *datagram-size*	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

Usage Guide N/A

Configuration Examples The following example configures 1,000 as the maximum length of the output sFlow datagram for sFlow Collector.

```
Ruijie(config)# sflow collector 1 max-datagram-size 1000
```

Verification Use the **show sflow** command to display the maximum length of the output sFlow datagram.

Prompt Messages N/A

Common Errors N/A

Platforms 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
collector-id	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 and aggregate ports.
sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Configuration Examples The following example enables interface TenGigabitEthernet 0/5 to send counter samples to sFlow Collector 2.

```
Ruijie(config-if-TenGigabitEthernet 0/5)# sflow counter collector 2
```

Verification Use the **show sflow** command to display the sFlow counter sampling configuration.

Prompt N/A

Messages

Common Errors N/A

Platforms 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
seconds	sFlow counter sampling interval. The range is form 3 to 2,147,483,647. The unit is second.

Defaults The default sFLow counter sampling interval is 30 seconds.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to configure the global sFlow counter sampling interval, and sFlow Counter sampling of all interfaces uses this sampling interval.

Configuration Examples The following example configures the sFlow counter sampling interval to 60 seconds.

```
Ruijie(config)# sflow counter interval 60
```

Verification Use the **show sflow** command to display the sFlow counter sampling interval.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

6.6 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

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.

Defaults Sending the flow 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 and aggregate ports.
sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Configuration Examples The following example enables interface TenGigabitEthernet 0/5 to send flow samples to sFlow Collector 2.

```
Ruijie(config-if-TenGigabitEthernet 0/5)# sflow flow collector 2
```

Verification Use the **show sflow** command to display the sFlow flow sampling configuration.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

6.7 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
length	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

6.8 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

Parameter Description

Parameter	Description
rate	Sampling rate of sFlow sampling. One packet is sampled from every *n* packets (*n* equals the value of **rate**). The range is from 4,096 to16,777,215.

Defaults The default sFlow flow sampling rate is 8,192.

Command Mode Global configuration mode

Default Level 14

Usage Guide 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.

Configuration Examples The following example sets the sFlow flow sampling rate to 4,096.

```
Ruijie(config)# sflow sampling-rate 4096
```

Verification Use the **show sflow** command to display the sFlow flow sampling rate.

Prompt Messages N/A

Common Errors N/A

Platforms N/A

6.9 sflow enable

Use this command to enable flow sampling and counter sampling on the interface.

sflow enable

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
N/A	N/A

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 and aggregate ports. sFlow datagram can be output only when an IP address is configured for the corresponding sFlow Collector.

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

6.10 show sflow

Use this command to display the sFlow configuration.
show sflow

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 sFlow configuration.

```
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. Currently, Ruijie supports V5 only.
Agent IP	IP address of the sFlow Agent. It can be configured by using the **sflow agent address** {*ip-address* | **ipv6** *ipv6-address* } command.
sflow counter 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 Colletor 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