RG-RSR20-X-28 Series Router

RGOS Command Reference, Release 10.4(3b75)

Copyright Statement

Exemption Statement

Preface

Thank you for using our products. This manual matches the RGOS Release 10.4(3b75).

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- Ruijie Networks Website: http://www.ruijienetworks.com/
- Service Email: service_rj@ruijienetworks.com
- Technical Support: http://www.ruijienetworks.com/service.aspx
- Technical Support Hotline: +86-4008-111-000

Related Documents

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

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
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

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

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

Basic Configuration Commands

CLI Authorization Commands

alias

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

alias *mode command-alias original-command*

no alias *mode*[*command-alias*]

Parameter Description

Parameter	Description
mode	Mode of the command represented by analias
command-alias	Alias of acommand
original-command	Syntax of the command represented by the alias

Defaults Some commands in privileged EXEC mode have default alias names.

Command Mode Global configuration mode

Usage Guide

The **help, ping, show, undebug**, and **undebug** commands havedefault aliasesh, **p**, **s**, **u**, and **un** in privileged EXEC mode.

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

An alias enables you touse 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 a command represented by an alias is the command mode existing in the current system. In global configuration mode, you can use the **alias ?**command to list allmodes under which you can configure aliases for commands.

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

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

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

For example, the default alias **s**representsthe **show**command in privileged EXEC mode. 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,

the following information is displayed if you set **sv** stand for the **show version** commandin privileged EXEC mode:

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

Analias 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
```

An alias also has its help information. For example, the following information is displayed if the alias **ia** represents **ip address** in the interface configuration mode:

```
Ruijie(config-if)# ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
Ruijie(config-if)# ip address
```

The preceding information lists the parameters of the**ip address**command 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 set in the system.

Configuration Examples

The following example uses the **def-route** command to represent the default route setting of **ip route0.0.0.0 0.0.0.0 192.168.1.1** in global configuration mode.

```
Ruijie# configure terminal
Ruijie(config)# alias config def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1
Ruijie(config)# def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
Ruijie(config)# end
Ruijie# show aliases config
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 alias settings.

Platform Description

N/A

privilege

Use the **privilege** command in global configuration modeto authorize the privilege level ofthe execution rightfora command. Use the **no** form of this command to restore the execution right 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	Indicates the CLI mode of the command to which the execution rightisauthorized.
all	Indicates the alias of acommand.
level *level*	Indicates the execution right level (0–15) of a command or sub-command.
reset	Restores the command execution right to the default values.
command-string:	Indicates the command string to be authorized.

Defaults N/A

Command Mode Global configuration mode

Usage Guide

The following table describes some keywords that can be authorized by the **privilege** command in CLI mode. The number of command modes that can be authorized may vary with devices. In 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
keychain	KeyChain configuration mode
keychain-key	KeyChain-key configuration mode
time-range	Time-Range configuration mode

Configuration Examples

The following example sets the password of CLI level 1 to **test** and authorize the **reload** rights to reset the device.

```
Ruijie(config)# enable secret level 1 0 test
```

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

Then, you can access the CLIas a level-1 user to use the **reload** command.

```
Ruijie> reload ?
LINE   Reason for reload
<cr>
```

The following example uses the keyword **all** to authorizeall sub-commands of reload to level-1 users:

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

Then, you can access the CLIas a 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 a CLI-level password.

Platform Description N/A

show aliases

Use the **show aliases** command in privileged EXEC mode to display all the command aliases or aliases in specifiedcommand modes.

show aliases [*mode***]**

Parameter Description

Parameter	Description
mode	Mode of the command represented by the alias

Defaults N/A

Command Mode PrivilegedEXEC mode

Usage Guide You can use this command to show all alias configurationsif nocommand mode has been entered.

Configuration Examples

The following example shows the command alias in privileged 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 the alias of a command.

Platform Description N/A

LINE Commands

access-class

Set the ACL (Access Control List) applied under Line. Use the **access-class** { *access-list-number* | *access-list-name* } **{ in | out }** command to configure the ACL under Line. Use the **no access-class** { *access-list-number* | *access-list-name* } {**in | out}** command to cancel the ACL configuration under LINE.

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 | *access-list-name*	Specifies the ACL defined by access-list
in	Performs access control over the incoming connections
out	Performs access control over the outgoing connections

Defaults

No ACL is configured under Line by default. All connections are accepted, and all outgoing connections are allowed.

Command Mode

Line configuration mode

Usage Guide

This command is used to configure ACLs under Line. All the incoming and outgoing connections are allowed, and no connection is filtered by default. After **access-class** is configured, only connections that pass access list filtering can be established. Use the **show running** command to view configuration information under Line.

Configuration Examples

Under line vty 0 4, configure access-list for the accepted connections to 10:

```
Ruijie# configure terminal
Ruijie(config)# line vty 0 4
Ruijie(config-line)# access-class 10 in
```

Related Commands

Command	Description
show running	Shows status information.

Version Description

line

Use the following command to enter the specified LINE mode:

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

Parameter Description

Parameter	Description
aux	Auxiliary port, on the routers generally.
console	Console port
tty	Asynchronous port, on the routers generally
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 Access to the specified LINE mode.

Configuration Examples Enter 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

line vty

This command is used to increase the number of VTY connections currently available. Use the **no** form of this command to decrease the number of currently available VTY connections.

line vty *line-number*

no line vty *line-number*

Parameter Description

Parameter	Description
N/A	N/A

Defaults There are five available VTY connections by default, numbered 0--4.

Command Mode	Global configuration mode
Usage Guide	To increase or decrease the number of available VTY connections, use the above commands.

Configuration Examples	Example 1: The following example increases the number of available VTY connections to 20. The available VTY connections are numbered 0-19.
	`Ruijie(config)# line vty 19`
	Example 2: The following example decreases the number of available VTY connections to 10. The available VTY connections are numbered 0-9.
	`Ruijie(config)# no line vty 10`

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

transport input

Use the **transport input** command to set the specified protocol under Line that can be used for communication. Use **default transport input** to restore the protocols under Line that can be used for communication to the default value.

transport input { all | ssh | telnet | none }

default transport input

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 under Line to be used for communication.

Defaults	VTY allows all the protocols to be used for communication by default. The default value of other types of TTYs is NONE, indicating that no protocols are allowed for communication. After some protocols are set available for communication, use the default transport input command to restore the setting to the default value.
Command Mode	Line configuration mode
Usage Guide	This command is used to set the protocols in the Line mode available for communication. By default,

VTY allows all the protocols for communication. After protocols available for communication are set, only these protocols can connect on the specific VTY successfully. Use the **show running** command to view configuration information under Line.

Note

You can restore the default configuration by using the **default transport input** command. The **no transport input** command is used to disable all the communication protocols in the LINE mode. The setting result is the same as that of **transport input none**.

Configuration Examples

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

```
Ruijie# configure terminal
Ruijie(config)# line vty 0 4
Ruijie(config-line)# transport input telnet
```

Related Commands

Command	Description
show running	Shows status information.

Version Description

System Upgrade and Maintenance Commands

Configuration Commands

This section describes how to perform system upgrade and maintenance by using the COPY command in the CLI environment of the main program.

To upgrade and maintain the system via the Xmodem protocol, run the **copy xmodem** command.

To upgrade and maintain the system via the TFTP protocol, run the **copy tftp** command.

To upload a local source file to or download a source file from the TFTP server, run the **tftp ipv6** command.

copy tftp

Use this command to upgrade and maintain the system via the TFTP protocol or to upload or download a file via the TFTP protocol.

copy flash: *filename* **tftp**:///*location/ filename*

copy tftp:// location*/filename* **flash**: *filename*

copy flash: *filename* **tftp**:///*location/ filename* **vrf** *vrfname*

copy tftp:// location*/filename* **flash**: *filename* **vrf** *vrfname*

Parameter Description

Parameter	Description
filename	File name
vrfname	VRF name

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide If the file is transferred successfully, the length of the file is displayed; otherwise, failure information is returned. Any files, such as main program files and parameter files, can be transferred via TFTP. TFTP transfer is implemented through network ports.

Configuration Examples Below are two examples: a) transfer a backup parameter file (**config.bak**) from the local host with the IP address of 192.168.12. 1 to the device; b) transfer a file (**switch.bin**) from the device to the local host whose IP address is 192.168.12.1:

```
Ruijie# copy tftp://192.168.12.1/config.bak flash:config.text
Ruijie# copy flash:switch.bin tftp://192.168.12.1/switch.bak
```

Related Commands	Command	Description
	N/A	N/A

Platform Description None

copy tftp ipv6

Use this command to perform the following operations:

- Download a file: Download a source file from the TFTP server to the local host.
- Upload a file:upload a local source file to the TFTP server.

This command is applicable to the IPv6 networking environment.

copy flash:*filename* **tftp**:// l*ocation* /*filename*

copy tftp:// location*/filename* **flash**: *filename*

Parameter Description	Parameter	Description
	filename	File name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example downloads the **config.text** file to the TFTP server.

```
Ruijie# copy tftp://[2000::100]/config.text
flash:config.text
Accessing tftp://[2000::100]/config.text...
Success : Transmission success,file length 1496
```

Related Commands	Command	Description
	N/A	N/A

Platform Description None

copy xmodem

Use this command to upgrade and maintain the system via the Xmodem protocol or to upload and download a file via the Xmodem protocol.

copy flash: *filename* **xmodem**

copy xmodem flash: *filename*

Parameter Description

Parameter	Description
filename	File name

Defaults

N/A

Command Mode

Privileged mode

Usage Guide

If the file is transferred successfully, the length of the file is displayed; otherwise, failure information is returned. Any files, such as main program files and parameter files, can be transferred via the Xmodem protocol. Xmodem transfer can only be implemented through out-of-band serial ports.
Below are two examples: a) transfer a file from the local host to the device via the Xmodem protocol; b) upload the configuration file on the device to the local host via the Xmodem protocol.

Configuration Examples

The following examples upload and download a file named **config.text**:

```
Ruijie# copy xmodem flash: config.text
Ruijie# copy flash: config.text xmodem
```

Related Commands

Command	Description
-	-

Platform Description

None

Switch Management Commands

disable

To switch from privileged EXEC mode to normal EXEC mode or lower the privilege level, run the **disable** command.

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 EXEC mode from privileged EXEC mode. If a new privilege level is added, the current privilege level will be lowered.


Note

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 EXEC mode enter to privileged EXEC mode or reaches a higher level of authority.

Platform Description N/A

enable

To enter privileged EXEC mode, run the normal user configuration command **enable**.

For details about the command, see the *Security Configuration Command Reference*.

Parameter

Parameter	Description

Description	N/A	N/A

Defaults For details, see the *Security Configuration Command Reference*.

Command Mode For details, see the *Security Configuration Command Reference*.

Usage Guide For details, see the *Security Configuration Command Reference*.

Configuration Examples For details, see the *Security Configuration Command Reference.*

Related Commands

Command	Description
N/A	N/A

Platform Description For details, see the *Security Configuration Command Reference*.

enable password

To configure passwords for different privilege levels, run the global configuration command **enable password**. The **no** form of this command is used to delete the password of a specified level.

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

no enable password [**level** *level*]

Parameter Description

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

Defaults N/A

Command Mode Global configuration mode

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

A valid password is defined as follows:

- A plaintext password consists of 1-26 upper/lower case letters and numbers.
- A cipher password only includes hexadecimal numbers: 0~9 and a~f/A~F.
- Leading spaces are allowed but usually ignored. Spaces in between or at the end are regarded as part of the password.


Caution

If encryption type is 7, the logical length of the cipher text you enter should be an even number.

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.

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 Description N/A

enable secret

To configure a security password for different privilege levels, run the global configuration command **enable secret**. The **no** form of this command is used to delete the password of a specified level.

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 caetgories: "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

enable service

To enable or disable a specified service such as **SSH Server/Telnet Server/Web Server/SNMP Agent**, use the **enable service** command in global configuration mode:

enable service { ssh-sesrver | telnet-server | web-server | snmp-agent}

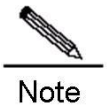
Parameter Description

Keyword	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	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.


Note

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	Views the service status in the current system.

Platform Description N/A

execute

To run the commands in batches, use the **execute** command in privileged EXEC mode.

run [**flash:**] *filename*

Parameter Description

Parameter	Description
flash:	Parent directory of the batch file
filename	Name of the batch file

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to run commands in batches.
You can define the filename and content of each batch file. When edited, the batch files on your computer are transferred to the flash memory of the device through TFTP. These batch files imitate user input, so you should edit the content in the order of CLI command configuration. For some

interactive commands, the response message should be pre-written into the batch files to ensure the commands can be normally rund.
Caution: The size of each batch file must not exceed 128 KB. Otherwise, the execution may fail. For over-sized batch files, you can divide them into several files smaller than 128 KB.

Configuration Examples

The following example runs the batch file **line_rcms_script.text**, which is used to enable the reverse **Telnet** function for all asynchronous interfaces with contents as follows:

```
configure terminal
line tty 1 16
transport input all
no exec
end
```

The execution result is as follows:

```
Ruijie# execute flash:line_rcms_script.text
executing script file line_rcms_script.text ......
executing done
Ruijie# configure terminal
Enter configuration commands, one per line.  End with  CNTL/Z.
Ruijie(config)# line tty 1 16
Ruijie(config-line)# transport input all
Ruijie(config-line)# no exec
Ruijie(config-line)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip http authentication

An Http Server requires logon authentication for access to a Web page. Use this command to set Web logon authentication mode.

ip http authentication {enable | local }

Parameter Description

Keyword	Description
enable	Uses the password set by the enable password or enable command. The password must be level 15. The system performs **enable** authentication by default.
local	Uses the username and password set by the local username command. The user must be bound to the privileges of level 15.

Defaults enable

Command Mode Global configuration mode

Usage Guide This command is used to set the mode of Web logon authentication. Use the **no ip http authentication** command to restore it to the default setting.

Configuration Examples The following example sets the mode of Web logon authentication as local:

```
Ruijie(Config)# ip http authentication local
```

Related Commands

Command	Description
enable service	Enables or disables the specified service.

Platform Description N/A

ip http port

To set an HTTP service port, use this command in global configuration mode:

ip http port *number*

Parameter Description

Keyword	Description
number	Port number of the HTTP server, 80 by default.

Defaults 80

Command Mode Global configuration mode

Usage Guide This command is used to set an HTTP service port. Use the **no ip http port** command to restore it to the default setting.

Configuration Examples The following example sets an HTTP service port as 8080:

```
Ruijie(Config)# ip http port 8080
```

Related Commands

Command	Description
enable service	Enables or disables the specified service.

Platform Description N/A

ip http source-port

This command is used to configure an HTTPS service port in global configuration mode.

ip http source-port *number*

Parameter Description

Parameter	Description
number	Configures an HTTPS service port, 443 by default.

Defaults 443

Command Mode Global configuration mode

Usage Guide This command is used to configure an HTTPS service port. The **no** form of this command is used to restore the default port configuration.

Configuration Examples The following example sets an HTTPS service port as 4443.

```
Ruijie(config)# ip http secure-port 4443
```

Related Commands

Command	Description
enable service	Enables or disables the specified service.
show web-server status	Shows the status of the web server.

Platform Description N/A

ip telnet source-interface

To specify the IP address of an interface as the source address for Telnet connection, use the **ip telnet source-interface** command in global configuration mode:

ip telnet source-interface *interface-name*

Parameter Description

Keyword	Description
interface-name	Specifies 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 specifies 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

lock

To set a temporary password for the terminal, run the **lock** command in EXEC mode .

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 show 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

lockable

To support the **lock** command at the terminal, run the **lockable** command in line configuration mode. The terminal does not support the **lock** command by default. Use the **no** command to cancel the setting.

lockable

no lockable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Line configuration mode

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

Configuration 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	Command	Description

Commands	lock	Locks the terminal.

Platform Description N/A

login

If AAA is disabled, run the **login** command to enable simple login password authentication on the interface. The **no** form of this command is used to delete the line login password authentication.

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 shows how to set 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

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. The **no** form of this command is used to delete the list.

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 shows how to associate 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

login local

If AAA is disabled, run the **login local** command to enable local user authentication on the interface. The **no** form of this command is used to delete the line for local user authentication.

login local

no login local

Parameter Description

Parameter	Description
N/A	N/A

Defaults **N/A**

Command Line configuration mode

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 shows how to set 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

privilege mode

See the “Configuring CLI Authorization Commands” chapter.

Parameter Description

Parameter	Description
N/A	N/A

Defaults See the “Configuring CLI Authorization Commands” chapter.

Command Mode See the “Configuring CLI Authorization Commands” chapter.

Usage Guide See the “Configuring CLI Authorization Commands” chapter.

Configuration Examples See the “Configuring CLI Authorization Commands” chapter.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

password

To configure a password for line login, run the **password** command. The **no** form of this command is used to delete the line login password.

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.

Note

If encryption type is 7, the logical length of the cipher text you enter should be an even number and the characters you entered must be in hexadecimal format: 0~9 and a~f/A~F.

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 the line login password as "red":Ruijie(config)# line vty 0
Ruijie(config-line)# password red
```

Related Commands

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

Platform N/A

Description

secret

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

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

no secret

Parameter Description

Parameter	Description
0	(Optional) specifies the plaintext password text and encrypts it with irreversible MD5 after configuration.
password	The password plaintext.
5 *encrypted-secret*	Specifies 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.

Caution 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 is used to set the password encrypted by irreversible MD5 for line login as vty0.

```
Ruijie(config)# line vty 0
Ruijie(config-line)# secret vty0
```

Related

Command	Description

Commands		
	login	Sets simple password authentication on the interface as the login authentication mode

Platform Description N/A

service password-encryption

To encrypt a password, run this command. The **no** form of this command is used to restore to the default value, but a password in cipher text cannot be restored to plain text.

service password-encryption

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

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

telnet

To log in a server that supports telnet connection, use the **telnet** command in EXEC (privileged) mode.

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 mode

Usage Guide This command is used to log in a telnet server.

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

Configuration Examples Example 1: 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
```

Example 2: 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	Shows the currently established Telnet sessions.
exit	Exits current connection.

Platform Description N/A

username

To set a local username, run the **username** command in global configuration mode.

username *name* {**nopassword** | **password** { *password* | [**0|7**]

encrypted-password }} **username** name **privilege** privilege-level

no username *name*

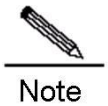
Parameter Description

Parameter	Description
name	Username
password	User password
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
privilege-level	User bound privilege level

Defaults N/A

Command Mode Global configuration mode

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



Note

If encryption type is 7, the logical length of the cipher text you enter should be an even number and the characters you entered must be in hexadecimal format: 0~9 and a~f/A~F.

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 bind the user to level 15.

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

Related Commands

Command	Description
login local	Enables local authentication

Platform Description N/A

username online amount

Use this command to set the simultaneously online amount of a local username. Use the no form of this command to clear restrictions on the amount.

username *name* **online amount** *numbers*

no username *name* **online amount**

Parameter Description

Parameter	Description
name	The username.
number	The simultaneously online amount of a local username within the range from 1 to 256.

Defaults The online amount of a local username simultaneously is not restricted.

Command mode Global configuration mode

Usage Guide After the simultaneously online amount of a local username is set, the number of clients logging in with the username must be within the specified range. When the number exceeds the limit, the username is not allowed to be used for login.

When the simultaneously online amount of a local username is set to 0, no login is allowed with the username by any client, including console login and remote login through this user.

Configuration Examples The following example shows how to set the simultaneously online amount that is allowed by admin, the local username, to 3.

```
Ruijie(config)# username admin online amount 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

username login mode

Use this command to set local username login mode. Use the **no** form of this command to clear restrictions on the login mode

username *name* **login mode { aux** | **console** | **ssh** | **telnet** }

no username *name* **login mode** { **aux** | **console** | **ssh** | **telnet** }

Parameter Description

Parameter	Description
name	The username.
aux	Confines local username login mode to aux.
console	Confines local username login mode to console.
ssh	Confines local username login mode to ssh.
telnet	Confines local username login mode to telnet.

Defaults Login mode of local username is not restricted.

Command mode Global configuration mode

Usage Guide This command is used to set local username login mode to one type or several types among aux, ssh and telnet. Only the configured login mode is allowed while the other modes are prevented.

Configuration Examples The following example shows how to set login mode of admin, the local username, as telnet.

```
Ruijie(config)# username admin login mode telnet
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

username secret

Use this command to set the local user's password encrypted by irreversible MD5 in global configuration mode.

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

no username *name* **secret**

Parameter Description

Parameter	Description
name	The username
0	(Optional) specifies the plaintext password text and encryptes it with irreversible MD5 after configuration.
password	The password plaintext.
5 *encrypted-secret*	Specifies the password text encrypted by irreversible MD5 and saves it as the encrypted password after configuration.

Defaults N/A

Command mode configuration mode

Usage Guide This command is used to set a username and a password text encrypted by irreversible MD5 for a local user.


Caution

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.

When the same user has set a “password” type password, the “secret” type password cannot be set. Only if the user clears the “password” type password can the “secret” type password be set, and vice versa.

When a user sets a “secret” password encrypted with irreversible MD5, it cannot be used for authentication protocols requiring passwords plaintext, such as CHAP. Currently there are two cases where the Ruijie device uses CHAP for authentication:

When a Ruijie device serves as the PPP authentication server, if CHAP is applied to authentication, the username configured with the “secret” type password cannot be used for authentication.

When a Ruijie device serves as the PPP authentication client, if CHAP is applied to authentication, the username configured with the “secret” type password cannot be used for authentication.

Configuration Examples The following example sets the username as test and configures a password encrypted by irreversible MD5.

```
Ruijie(config)# username test secret 0 pw15
```

After configuration, pwd15 will perform irreversible MD5 encryption and the outcome is shown with the **show** command as follows:

```
username test secret 5 $1$323T$A7q8FF9xy6rrF3r6
```

Related Commands

Command	Description
login local	Selects local authentication as the authentication mode in line mode.

Platform Description N/A

banner login

To configure the login banner, run the **banner login** command in clobal configuration mode. Use the **no banner login** command to remove the configuration.

banner login *c message c*

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 shows how to configure the login banner:

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

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

banner motd

To set the Message-of-the-Day (MOTD), run the **banner motd** command in global configuration mode. To delete the MOTD setting, run the **no banner motd** command.

banner motd c message c

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 shows the configuration of MOTD:

```
Ruijie(config)# banner motd $ hello,world $
```

Related Commands

Command	Description
-	-

Platform Description N/A

boot config

This command is used to set a boot configuration filename for the device. The **no** form of this command is used to delete the filename.

boot config prefix:/[directory/]filename

no boot config

Parameter Description

Parameter	Description
prefix:	Prefix of file system type. Note that prefix can be used to locate and access files in V10.4(2) or later versions. Refer to the File System Configuration Guide for details.
/[directory/]filename	File directory and filename

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to specify the device's boot configuration filename. When booting the device, the system loads the configuration file as follows:

- If no service config command is available, configuration files are loaded in the following sequence: boot configuration filenames configured using the boot config command, flash:/config.text, network boot configuration filenames configured using the boot network command, and the default configuration (null configuration).
- If a service config command is available, configuration files are loaded in the following sequence: network boot configuration filename configured using the boot network command, boot configuration filename configured using the boot config command, flash:/config.text, and the default configuration (null configuration).
- During the loading process, the system will not load another configuration file until one is successfully loaded.

This function can be used for fast failure recovery when the device's main configuration file is damaged.


Caution As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.
This command is only supported on the RSR20, RSR30, R2700 V5.0, RSR50, RSR50E, and NPE50 series of routers and the S86 series of switches.

Configuration Examples The following example sets the device's boot configuration filename as "flash:/config_main.text":

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

Related Commands

Command	Description
boot network	Sets the device's network boot configuration filename.
service config	Allows the device to first download the boot configuration file from a remote network server.
show boot	Shows the device's boot configuration.

Platform Description N/A

boot ip

This command is used to configure a local IP address for TFTP transfer during device booting. The **no** form of this command is used to delete the configuration.

boot ip local-ip [**gateway** gateway-ip **mask** mask-ip]

no boot ip

Parameter Description

Parameter	Description
local-ip	Local IP address for TFTP transfer during device booting.
gateway-ip	Gateway IP address for TFTP transfer during device booting.
mask-ip	Mask IP address for TFTP transfer during device booting.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure a local IP address for TFTP transfer during device booting. When the device is booting, the system uses this IP address as the local IP address for TFTP transfer. If a

gateway and mask are also used, and the local IP address and gateway IP address are not in the same network segment, TFTP uses the gateway for file transmission during system booting.


Caution

The system downloads the remote TFTP file configured by using the **boot network** or **boot system** command during system booting only when the **boot ip** command is correctly configured.

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

This command is only supported on the RSR20, RSR30, R2700 V5.0, RSR50, RSR50E, and NPE50 series of routers and the S86 series of switches.

Configuration Examples

The following example configures a local IP address for TFTP transfer during device booting:

```
Ruijie(config)# boot ip 192.168.7.11
```

Related Commands

Command	Description
show boot	Shows the boot configuration of the device.

Platform Description

N/A

boot network

This command is used to set the network boot configuration filename for the divice. The **no** form of this command is used to delete the filename.

boot network tftp:// l*ocation* / *filename*

no boot network

Parameter Description

Parameter	Description
location	Address of the TFTP server.
filename	Filename on the TFTP server.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to specify the device's network boot configuration filename. When booting the device, the system loads the configuration file as follows:

- If no service config command is available, configuration files are loaded in the following sequence: boot configuration filename configured using the boot config command,

flash:/config.text, network boot configuration filename configured using the boot network command, and the default factory-delivered configuration (null configuration).

- If a service config command is available, configuration files are loaded in the following sequence: network boot configuration filename configured using the boot network command, boot configuration filename configured using the boot config command, flash:/config.text, and the default factory-delivered configuration (null configuration).
- During the loading process, the system will not load another configuration file until one is successfully loaded.

This function can be used for fast failure recovery when the device's master configuration file is damaged.


Caution

You should use the **boot ip** command to correctly configure the local IP address for device booting before the system can download the remote file through TFTP. Otherwise, TFTP transfer may fail during booting.

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

This command is only supported on the RSR20, RSR30, R2700 V5.0, RSR50, RSR50E, and NPE50 series of routers and the S86 series of switches.

Configuration Examples The following example configures the network boot configuration filename for the device:

```
Ruijie(config)# boot network tftp://192.168.7.24/config.text
```

Related Commands

Command	Description
boot config	Sets the device's boot configuration filename.
boot ip	Configures the local IP address for TFTP transfer during device booting.
service config	Allows the device to first download the boot configuration file from a remote network server.
show boot	Shows the boot configuration of the device.

Platform Description N/A

boot system

This command is used to set a filename for the device's main startup program and specify the boot priority. The **no** form of this command is used to delete the filename of the main program corresponding to the priority.

boot system *priority* prefix:/[directory/]filename

no boot system [*priority*]

Parameter Description

Parameter	Description
priority	Boot priority of a main program, in the range of 1 to 10, with 1 as the highest priority.
prefix:	Prefix of the file system. Note that prefix can be used to locate and access files in V10.4(2) or later versions. Refer to the *File System Configuration Guide* for details.
/[directory/]filename	Filename of a main program used for booting. Note that when the prefix is used to locate a file, the directory following ":" should be an absolute path.

Defaults The default filename of the main startup program is *flash:/rgos.bin*, with the priority as 5.

Command Mode Global configuration mode

Usage Guide This command can be used to set filenames for multiple main programs used for booting and specify the boot priority. The system will attempt to boot the main programs according to their priority levels in the descending order (1 as the highest and 10 as the lowest priority) during the boot stage. This function can be used for fast failure recovery when the device's main program is damaged.


Caution

You should use the **boot ip** command to correctly configure the local IP address used by the device during booting, before the system can download the remote file through TFTP. Otherwise, TFTP transfer will fail during booting. When using TFTP, make sure the device's built-in flash memory has enough space for the boot file. The boot file is saved in the built-in flash memory as a hidden file during booting and will be deleted before the next boot.

The **no boot system** *[priority]* command can be used to delete the configured name of the main program corresponding to the boot priority level. If the priority parameter is not set, the configured filenames of all main startup programs will be deleted.

If the **no boot system** command is used to delete all the configured filenames of main startup programs and no filenames of main startup programs are configured, the system will automatically recover the default configuration (filename of the main program is "flash:/rgos.bin" with the priority level of 5) during the next boot.

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

Configuration Examples Example 1: Configure the name of the main program as "flash:/rgos.bin" and the name of the backup main program as "flash:/rgos_bak.bin".

```
Ruijie(config)# boot system 5 flash:/rgos.bin
Ruijie(config)# boot system 8 flash:/rgos_bak.bin
```

As "flash:/rgos.bin" has a higher priority, the device will boot from this file first. If "flash:/rgos.bin" is

damaged, which results in booting failure, the system will automatically boot from "flash:/rgos_bak.bin" with a lower priority.

Example 2: Configure the system to boot from a TFTP server.

```
Ruijie(config)# boot system 9 tftp://192.168.7.24/rgos.bin
```

Example 3: Configure the system to boot from a USB drive.

```
Ruijie(config)# boot system 1 usb1:/rgos.bin
```

Example 4: Delete the configured filename of the main program corresponding to priority 8.

```
Ruijie(config)# no boot system 8
Delete boot system config: [Priority: 8; File Name: flash:/rgos_bak.bin]? [no]
yes
```

Example 5: Delete all configured filenames of main startup programs.

```
Ruijie(config)# no boot system
Clear ALL boot system config? [no] yes
```

Related Commands

Command	Description
show boot	Shows the boot configuration of the device.
boot ip	Configures the local IP address for TFTP transfer during device booting.

Platform Description This command is only supported on the RSR20, RSR30, R2700 V5.0, RSR50, RSR50E, and NPE50 series of routers and the S86 series of switches while not supported on RSR10 series routers.

boot system

Use this command to set the main startup program filename for the device. The **no** form of this command restores the filename to the default setting.

boot system *url*

no boot system

Parameter Description

Parameter	Description
url	Address used for booting files.

Defaults The default filename is *flash:/rgos.bin*.

Command Mode Global configuration mode

Usage Guide This command is used to set the main startup program filename for the device. The system boots

from the file specified by the url parameter. This function alllows you to switch quickly between different software versions.

Caution

1. This command only supports the URL with flash prefix, that is, it can only set the file in local flash memory as the startup-config filename.
2. This configuration must be used in early boot stage, so it is saved in the Boot ROM of the device instead of the configuration file.

Configuration Examples

The following example sets the main program filename for the device to quickly switch between different software versions.

```
Ruijie#show boot system
system boot file: flash:/rgos.bin
```

```
Ruijie#dir
Directory of flash:/
   11015744 2008-01-01 08:00:46  rgos.bin
   12019754 2008-02-01 08:00:46  s5750_10_4.bin
       399 2006-01-01 08:01:37  config.text
33,030,144 bytes total. (10,590,592 bytes free)
```

```
Ruijie(config)# boot system s5750_10_4.bin
Ruijie(config)# show boot system
system boot file: flash:/ s5750_10_4.bin
```

When the device restarts, the system boots from *s5750_10_4.bin*.

Related Commands

Command	Description
show mainfile	Shows configuration information about equipment booting.

Platform Description

This command is supported on Ruijie devices except for RSR10, RSR20, RSR30, R2700 V5.0, RSR50, RSR50E, and NPE50 series of routers and the S86 switch series.

clock set

To configure system clock manually, run one of the two formats of the **clock set** command in privileged EXEC mode:

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.
Currently, the following networking devices do not support hardware clock: S2026G, S2026F, S2028, and RSR10.

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	Shows current clock.

Platform Description N/A

clock update-calendar

In privileged EXEC mode, use the **clock update-calendar** 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 This command is not supported on the S2026G, S2026F, S2028, and RSR10.

exec-timeout

To configure connection timeout for this device in LINE mode, use the **exec-timeout** command. Once the connection timeout in LINE is cancelled by using the **no exec-timeout** command, the connection never expires.

exec-timeout minutes [seconds]

no exec-timeout

Parameter Description

Parameter	Description
minutes	Timeout in minutes.
seconds	(Optional) Timeout in minutes

Defaults The default timeout 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 specifies the connection timeout as 5’30’’.

```
Ruijie(config-line)#exec-timeout 5 30
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

hostname

To specify or modify the hostname of a device, run the **hostname** command in global configuration mode**.**

hostname *name*

Parameter Description

Parameter	Description
name	Device hostname, string, number or hyphen, up to 63 characters.

Defaults The default hostname 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 Examples The following example configures the hostname of the device as BeiJingAgenda:

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

prompt

To set the **prompt** command, run the **prompt** command in global configuration mode. To delete the prompt setting, run the **no prompt** command.

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 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

reload

To restart the device system, run the privileged user command **reload**.

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 of 1 to 31
year	Year in the range of 1993 to 2035. No abbreviation is allowed.
cancel	Cancels the scheduled restart.

Defaults N/A

Command Mode Privileged EXEC 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

service config

This command is used to enable the device to first download the boot configuration file from a remote network server. The **no** form of this command is used to disable this function.

service config

no service config

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command Mode Global configuration mode

Usage Guide This command must be used together with the boot config and boot network commands. When booting the device, the system loads the configuration file as follows:

- If no service config command is available, configuration files are loaded in the following sequence: boot configuration filename configured using the boot config command, flash:/config.text, network boot configuration filename configured using the boot network command, and the default factory-delivered configuration (null configuration).
- If a service config command is available, configuration files are loaded in the following sequence: network boot configuration filename configured using the boot network command, boot configuration filename configured using the boot config command, flash:/config.text, and the default factory-delivered configuration (null configuration).

During the loading process, the system will not load another configuration file until one is successfully loaded.

As this command configuration is used by the system in the early boot stage, the configuration is saved in the device Boot ROM instead of the configuration file.

This command is only supported on the RSR20, RSR30, R2700 V5.0, RSR50, RSR50E, and NPE50 series of routers and the S86 series of switches.

Configuration Examples

The following example enables the device to first download the boot configuration file from a remote network server and configure the network boot configuration filename:

```
Ruijie(config)# service config
Ruijie(config)# boot network tftp://192.168.7.24/config.text
```

Related Commands

Command	Description
boot config	Sets the boot configuration filename for the device.
boot network	Sets the network boot configuration filename for the device.

Platform Description

N/A

session-timeout

To configure the session timeout for a remote terminal in current LINE mode, use the **session-timeout** command. When the session timeout for the remote terminal in LINE mode is cancelled, 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 min.

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

Command	Description

Commands	N/A	N/A

Platform Description N/A

speed

To set the speed at which the terminal transmits packets, run the **speed** *speed* command in line configuration mode. To restore the speed to its default, run the **no speed** command.

speed *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 rate 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 shows how to set 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

write

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

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

Parameter

Parameter	Description

Description

memory	Writes the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**.
network	Saves the system configuration to the TFTP server, which is equivalent to **copy running-config tftp**.
terminal	Shows the system configuration, which is equivalent to **show running-config**.

Defaults

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.

Caution

On a device that enables you to specify a boot configuration file, use the **write** [**memory**] command to do the following:

- If you have not specified a boot configuration file using the **boot config** command, the system stores configurations in **/config.text** in the built-in flash memory by default.
- If you have specified a boot configuration file using the **boot config** command, the system stores configurations in the file.
- If you have used the **boot config** command to specify a boot configuration file but the file does not exist:
  - 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 the default boot configuration file **/config** 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.

The **boot config** command is supported only on the RSR10, RSR20, R2700 V5.0, RSR50, and NPE50 series of routers.

Configuration Examples

Example 1: The following example shows how to save system configuration on a device that does not support **boot config**.

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

Example 2: The following example shows how to use the **write** command on a device that supports **boot config** before and after removing a USB drive you have set up to store the boot configuration file:

```
Ruijie(config)# boot config /mnt/usb1/config.text
Ruijie# write
Building configuration...
Write to boot config file: [/mnt/usb1/config.text]
[OK]
Ruijie# usb remove 1
0:1:1:38 Ruijie: USB-5-USB_DISK_REMOVED: USB Device <USB Mass Storage Device>
Removed!
Ruijie# write
Building configuration...
Write to boot config file: [/mnt/usb1/config.text]
[Failed]
The device [usb1] does not exist, write to the default config file
[/config.text]? [no] yes
Write to the default config file: [/config.text]
[OK]
```

Related Commands

Command	Description
boot config	Names the boot configuration file on the device.
copy	Copies device configuration files.
show running-config	Views the system configuration.

Platform Description N/A

show boot

Use this command to show the device boot configuration.

show boot {config | network |system | ip}

Parameter Description

Parameter	Description
config	Shows the configuration of the startup-config filename.
network	Shows the configuration of the network startup-config filename.
system	Shows the configuration of the main startup program filename.
ip	Shows the configuration of local IP address used in the device starting.

Defaults

Command Privileged EXEC mode

Mode

Usage Guide This command is used to show the current boot configuration of the device.

Note

The size and modification time are not shown for files on a remote TFTP server. The size and modification time are shown as N/A for such files.

When the **show boot system** command is used, the file size and modification time are shown as “N/A” if no main program is found.

Configuration Examples

1.The following example shows the configuration of the startup-config filename:

```
Ruijie# show boot config
Boot config file: [/config_main.text]
Service config: [Disabled]
```

2.The following example shows the configuration of network startup-config filename:

```
Ruijie# show boot network
Network config file: [tftp://192.168.7.24/config.text]
Service config: [Enabled]
```

3.The following example shows the configuration of the main program filename and boot priority:

```
Ruijie# show boot system
Boot system config:
================================================
Prio     Size             Modified  Name
---- --------- ------------------- -----------------
 1
 2
 3
 4
5     3205120 2008-08-26 05:22:46 flash:/rgos.bin
6
7
8     3205120 2008-08-26 05:25:09 flash:/rgos_bak.bin
9          N/A                 N/A tftp://192.168.7.24/
                                  rgos.bin
10
================================================
```

4.The following example shows the configuration of local IP address that used in the device starting:

```
Ruijie# show boot ip
System boot ip: [192.168.7.11]
```

```
System boot gateway: N/A
System boot mask: N/A
```

Related Commands	Command	Description
	N/A	N/A

Platform Description This command is supported only on RSR10, RSR20, RSR30, R2700 V5.0, RSR50, RSR50E, and NPE50 series of routers and the S86 switch series.

show mainfile

This command is used to show the current filename of the main startup program.

show mainfile

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to show the current filename of the main startup program.

Configuration Examples

```
Ruijie# show mainfile
MainFile name: /rgos.bin
```

Related Commands	Command	Description
	boot system	Sets the filename of the main startup program.

Platform Description This command is not supported and not visible on Ruijie devices except on RSR10, RSR20 and RSR30 serious routers.

show clock

To view the system time, run the **show clock** command in privileged EXEC mode.

show clock

Parameter	Parameter	Description

Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to view the current system clock.

Configuration Examples The following example shows 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

show line

To show the configuration of a line, run the **show line** command in privileged EXEC mode.

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

Parameter Description	**Parameter**	**Description**
	console	Shows the configuration of a console line.
	aux	Checks configuration information relating to the aux line.
	vty	Shows the configuration of a vty line.
	line-num	Number of the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

This command shows the configuration of a line.

Configuration Examples The following example shows 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    N/A       ^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

show reload

To show the system restart settings, run the **show reload** command in privileged EXEC mode.

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 show the restart settings of the system.

Configuration Examples The following example shows 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 Commands	Command	Description
	N/A	N/A

Platform Description N/A

show running-config

To show how the current device system is configured, run the **show running-config** command in privileged EXEC mode.

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

show startup-config

To view the device configuration stored in the Non Volatile Random Access Memory (NVRAM), run the **show startup-config** command in privileged EXEC mode.

show startup-config

Parameter	Parameter	Description

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

show version

To view information about the system, run the **show version** command in privileged EXEC mode.

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 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 shows 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 The complete parameters such as devices and module are not supported on RSR10, RSR20 or RSR30 serious routers.

show web-server status

This command is used to show the configuration and status of a web server.

show web-server status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows a result of the **show web-server status** command:

```
Ruijie# show web-server status
http server status : enabled
http server port : 80
```

```
https server status:  enabled
https server port: 443
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Network Connectivity Test Tool Commands

ping

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* | **ip**] [*ip-address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**]]

Parameter Description

Parameter	Description
vrf-name	VRF name
ip-address	Specifies an IPv4 address.
length	Specifies the length of the packet to be sent.
times	Specifies the number of packets to be sent.
seconds	Specifies the timeout time.
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 no segmentation to the datagrams. By default, the DF bit is 0.
validate	Sets whether to validate the reply packets.

Defaults

Five packets with 100 Byte in length are sent to the specified IP address within the specified time (2 seconds by default).

Command Mode

Privileged EXEC mode

Usage Guide

The ping command can be used in ordinary and privileged EXEC modes. In ordinary EXEC mode, only the basic functions of ping are available. In 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 100 Byte 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, which can be performed only in privileged EXEC mode, 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 specific configuration, refer to the DNS Configuration section. The VRF function is provided only in the RSR devices.

Configuration Examples

The following example shows the ordinary ping.

```
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 following example shows the extension ping.

```
Ruijie# ping 192.168.5.197 length 1500 ntimes 100 timeout 3 data ffff source
192.168.4.10
 Sending 100, 1500-byte ICMP Echoes to 192.168.5.197, 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

Command	Description
N/A	N/A

Platform Description

The command is supported by all devices.

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 [**ipv6**] [*ip-address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*]]

Parameter Description

Parameter	Description
ip-address	Specifies an IPv6 address.
length	Specifies the length of the packet to be sent.
times	Specifies the number of packets to be sent.
seconds	Specifies the timeout time.
data	Specifies the data to fill in.
source	Specifies the source IPv6 address or the source interface. The loopback interface address (for example: ::1) is not allowed to be the source address.

Defaults

Five packets with 100Byte in length are sent to the specified IP address within the specified time (2s by default).

Command Mode

Privileged EXEC mode

Usage Guide The ping ipv6 command can be used in ordinary and privileged EXEC modes. In ordinary mode, only the basic functions of ping ipv6 are available. In privileged 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 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 specific configuration, refer to the DNS Configuration section.

Configuration Examples The following example shows the ordinary ping ipv6.

```
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 following example shows the extension ping ipv6.

```
Ruijie# ping ipv6 2000::1 length 1500 ntimes 100 timeout 3 data ffff source
2000::2
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 Commands

Command	Description
N/A	N/A

Platform Description	The command is supported by all ipv6-supported devices.

traceroute

Use the **traceroute** command to show all gateways passed by the test packets from the source address to the destination address.

traceroute [**vrf** vrf-name | **ip**] [ip-address [ip-adress [**probe** number] [**source** source] [**timeout** seconds] [**ttl** minimum maximum]]

Parameter Description

Parameter	Description
vrf-name	VRF name
Ip-address	Specifies an IPv4 address.
number	Specifies the number of probe packets to be sent.

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.
minimum maximum	Specifies the minimum and maximum TTL values.

Defaults N/A

Command Mode Privileged EXEC mode

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 specific configuration, refer to the DNS Configuration part. The VRF function is provided only in the RSR devices.

Configuration Examples The following is two examples that apply **traceroute**, the one is of the smooth network, and the other is the network in which some gateways are not 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 is 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 shows that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) 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 The command is supported by all devices. Where, the VRF function can only be provided in the RSR device.

traceroute ipv6

Use this command to show all gateways passed by the test packets from the source address to the destination address.

traceroute [**ipv6**] [*ip-address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

Parameter Description

Parameter	Description
Ip\-address	Specifies an IPv6 address or a domain name.
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 N/A

Command Mode Privileged EXEC mode

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 specific configuration, refer to the DNS Configuration part.

Configuration Examples The following is two examples that apply **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 is 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 gateway 4 fails.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

File System Commands

cd

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

cd [*filesystem:*][*directory*]

Parameter Description

Parameter	Description
filesystem:	Specified file system. This parameter must carry ":".
directory	Specified directory

Defaults The default directory is the flash root directory.

Command Mode Privileged EXEC mode

Usage Guide This command will change the current path or directory of the file system. If a relative path is used by other commands of the file system, that is the path does not begin with "/", it is the current path related to the system. Use the pwd command to view the present directory.

Configuration Examples

Example 1: The following example sets the root directory of usb0 as the present directory:

```
Ruijie# cd usb0:/
```

Example 2: The following example sets the root directory of the sd card as the present directory:

```
Ruijie# cd sd0:/
```

Related Commands

Command	Description
pwd	Shows the present file directory.

Platform Description N/A

copy

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

copy *source-url destination-url*

Parameter Description

Parameter	Description
source-url	Source file URL, which can be local or remote based on

	whether the file is uploaded or downloaded.
destination-url	Destination file URL, which can be local or remote based on whether the file is uploaded or downloaded.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

This command is used to copy files among various local storage media and to transmit files between network servers:

The following table lists URL prefixes for specific file system:

Prefix	Description
flash:	Flash storage media. This prefix can be used in all devices. The default is flash if the URL uses no prefix. Generally, the bootstrap main program is stored in the flash.
tftp:	TFTP network server
xmodem:	Uses the xmodem protocol to send or receive files to or from network devices.
slave:	Flash on the secondary board from the chassis device
usb0:	The first USB device
usb1:	The second USB device
sd0:	The first SD card
sw1-m1-disk0:	Management board on the M1 slot of the chassis with switch id 1, in the VSU mode
sw1-m2-disk0:	Management board on the M2 slot of the chassis with switch id 1, in the VSU mode
sw2-m1-disk0:	Management board on the M1 slot of the chassis with switch id 2, in the VSU mode
sw2-m2-disk0:	Management board on the M2 slot of the chassis with switch id 2, in the VSU mode

This command does not support the wildcard.

No specified URL prefix refers to the current file system by default.

Configuration Examples

Example 1: The following example downloads a file from the tftp server:

```
Ruijie# copy tftp://192.168.201.54/rgos.bin flash:/
```

Example 2: The following example uploads a file to the tftp server:

```
Ruijie# copy flash:/rgos.bin tftp://192.168.201.54/rgos.bin
```

Example 3: The following example uses the xmodem protocol to download a file:

```
Ruijie# copy xmodem: flash:/config.text
```

Example 4: The following example copies a file to the flash disk:

```
Ruijie#copy flash:/config.text usb0:/config.text
```

Example 5: The following example copies a file to the secondary management board:

```
Ruijie#copy flash:/config.text slave:/config.text
```

Example 6: The following example copies a file from the flash to the SD card:

```
Ruijie#copy flash:/rgos.bin sd0:/rgos.bin
```

Example 7: The following example copies a file from the flash disk to the SD card:

```
Ruijie#copy usb0:/config.text sd0:/config.text
```

Example 8: The following example copies a file from the SD card to the flash disk:

```
Ruijie#copy sd0:/config.text usb0:/config.text
```

Related Commands

Command	Description
delete	Deletes a file.
rename	Renames a file.
dir	Shows the file list of the specified directory.

Platform Description

N/A

delete

Use this command to delete files.

delete [recursive] *url*

Parameter Description

Parameter	Description
recursive	Non-empty directories to be deleted.
url	URL of the file to be deleted

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to delete the specified file in the URL. This command can delete files stored in the local storage media, that is, the URL must be flash:/ usb0:/ or usb1:/ slave:/. If no prefix is specified in the URL, it will delete files in the current file system.

Note This command does not support wildcard.

Configuration Examples

Example 1: The following example deletes `tmpfile` from the present directory:

```
Ruijie# delete tmpfile
```

Example 2: The following example deletes `rgos.bin.bak` from the secondary board:

```
Ruijie# delete slave:/rgos.bin.bak
```

Example 3: The following example deletes `aaa.bin` form the SD card:

```
Ruijie# delete sd0:/aaa.bin
```

Example 4: The following example deletes a non-empty directory aaa on the FLASH:

```
Ruijie# delete recursive aaa
```

Related Commands

Command	Description
copy	Copies a file.
dir	Shows the file list of the specified directory.

Platform Description

The devices locating files through URL such as S86 and S12000 distributed devices support URL parameters (to locate files) and does not support deleting the non-null directory recursively (recursive parameters are not supported).

dir

Use this command to show files in the present directory.

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

Parameter Description

Parameter	Description
filesystem	Sets the file system for the file to be displayed. This parameter must carry ":".
directory	Sets the directory for the file to be displayed.

Defaults

Information of files under the present path is shown by default.

Command Mode

Privileged EXEC mode

Usage Guide

Enter the specified directory to show information of all files in that directory. If no parameter is specified, information of files in the present directory is shown by default.

Note This command does not support wildcard.

Configuration

Example 1: The following example shows file information of the root directory in the secondary

Examples

board:

```
Ruijie# dir slave0:/
Directory of slave:/
   Mode Link     Size             MTime Name
-------- ---- --------- ------------------- ------------------
          1  10838016 2008-01-01 00:01:53 rgos.bin
          1      399 2008-01-01 00:01:37 config.text
          1      399 2008-01-01 00:17:58 cfg.txt
-----------------------------------------------------------------
3 Files (Total size 11210782 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20463616 bytes (19MB) available.
```

Example 2: The following example shows information of all files in the present directory:

```
Ruijie# dir
Directory of temp:/
   Mode Link     Size             MTime Name
-------- ---- --------- ------------------- ------------------
          1      399 2008-01-01 00:17:58 a.dat
-----------------------------------------------------------------
1 Files (Total size 399 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20463616 bytes (19MB) available.
```

Related Commands

Command	Description
pwd	Shows the present directory.
cd	Sets the present directory of the file system.

Platform Description

N/A

mkdir

Use this command to create a directory.

mkdir *directory*

Parameter Description

Parameter	Description
directory	Name of the directory to be created

Defaults

N/A

Command Mode

Privileged EXEC mode

Enter the name of the directory to be created (including the path).

Usage Guide


Note

If the created folder already exists, the creation will fail. If the upper-level directory for the directory to be created does not exist, the specified directory cannot be created. For example, if the directory flash:/backup does not exist, the directory flash:/backup/temp cannot be created. The solution is to create the directory flash:/backup first and then to create the directory flash:/backup/temp.

Configuration Examples

Example 1: The following example creates the test directory at the root directory:

```
Ruijie# mkdir test
```

Example 2: The following example creates the test2 directory under the root directory of the SD card:

```
Ruijie# mkdir sd0:/test2
```

Related Commands

Command	Description
rmdir	Deletes a directory.
pwd	Shows the present directory.

Platform Description

N/A

rename

Use this command to move or rename the specified file.

rename *url1 url2*

Parameter Description

Parameter	Description
url1	URL of the source file to be moved
url2	URL of the destination file or directory

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command can rename files under the same directory or move files between different storage media. It can only move local files, but cannot transfer files to the server using the protocol. The supported prefixes include: usb0/1, flash and slave.

Configuration Examples

Example 1: The following example moves the `log.txt` to the upper-level directory and rename it `config.txt`:

```
Ruijie# rename tmp/log.txt ../config.txt
```

Example 2: The following example moves the `log.txt` in the secondary board to the usb0 device:

```
Ruijie# rename slave:/log.txt usb0:/log.txt
```

Example 3: The following example renames the `log.txt` in the present directory as `log.txt.bak`:

```
Ruijie# rename log.txt log.txt.bak
```

Example 4: The following example moves the `rgos.bin` in the SD card to the flash:

```
Ruijie# rename sd0:/rgos.bin flash:/rgos_bak.bin
```

Example 5: The following example moves the `test.txt` in the flash disk to the SD card:

```
Ruijie# rename usb0:/test.txt sd0:/test2.txt
```

Related Commands

Command	Description
delete	Deletes files.
copy	Copies files.

Platform Description

N/A

rmdir

Use this command to delete an directory.

rmdir *directory*

Parameter Description

Parameter	Description
directory	Name of the directory to be deleted, which must be empty.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command does not support wildcard, and the directory to be deleted must be empty.

Configuration Examples

If there is a tmp directory in the present directory and the directory is empty:

```
Ruijie# rmdir tmp
```

Related Commands

Command	Description
mkdir	Creates a directory.

Platform Description N/A

pwd

Use this command to show the working path.

Pwd

Parameter Description

Parameter	Description
None	

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command shows the present working path.

Configuration Examples The following example shows the present working path.

```
Ruijie# pwd
flash:/
```

Related Commands

Command	Description
cd	Changes the file system's present directory.

Platform Description N/A

show file systems

Use this command to show the file system information.

show file systems

Parameter

Parameter	Description

Description	None	

Defaults N/A

Command Mode N/A

Usage Guide Use this command to show file systems supported in the present device and available spaces of the file systems.

Configuration Examples Example 1: The following example shows the file system information:

```
Ruijie# show file systems
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Syslog Commands

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 **None**

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	Shows the logs in the buffer.
logging buffered	Records the logs in the memory buffer.

Platform Description None

more flash

Use this command to show the contents of the logs stored in the extended FLASH in privileged EXEC mode.

more flash: *filename*

Parameter Description

Parameter	Description
filename	Log file name.

Defaults None

Command Mode	Privileged EXEC mode
Usage Guide	In the extended FLASH, the log file indicates the files with the prefix "//f2/", "//f3/'. This command only allows you to view the log files. You cannot use this command to view other non-log files.

Configuration Examples	The following example shows the results of the log files in the extended FLASH:
	`Ruijie# more flash://f2/log.txt`
	`look up file in the extended flash://f2/log.txt`
	`00004 2004-11-17 4:1:32 Ruijie: %5:Reload requested by Administrator. Reload Reason :Reload command`

Related Commands

Command	Function
logging file flash	Records the logs to the extended FLASH.

Platform Description	None

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 memory buffer size to the default value.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

Parameter Description

Parameter	Description
bufferN/Asize	Size of the buffer is related to the specific device type: 1. For the kernel / aggregation switches, 4 K to 10 M bytes. 2. For the access switches, 4 K to 1 M. 3. For other devices, 4 K to 128 K Bytes.
level	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.

Defaults	The buffer size is related to the specific device type. 1. kernel switches: 1 M Bytes; 2. aggregation switches: 256 K Bytes; 3. access switches: 128 K Bytes; 4. other devices: 4 K Bytes

The log severity is 7.

Command Mode Global configuration mode

Usage Guide The memory buffer for log is used in recycled manner. That is, when the memory buffer with the specified size is full, the oldest information will be overwritten. To show the log information in the memory buffer, run the **show logging** command in privileged EXEC 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 EXEC 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.

Caution 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	Shows the logs in the buffer.
clear logging	Clears the logs in the log buffer.

Platform Description None

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 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	Shows the logs and related log configuration parameters in the buffer.

Platform Description None

logging count

Use this command to enable the log statistics function in global configuration mode. Use the **no** form of the command to delete the log statistics and disable the statistics function.

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 Enable the log statistics function:

```
Ruijie(config)# logging count
```

Related Commands

Command	Description
show logging count	Views log information about modules of the system.
show logging	Views basic configuration of log modules and log information in the buffer.

Platform Description None

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 it to the default device value (23).

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 Local7(23)

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 None

logging file flash

Use this command to record logs in the extended flash in global configuration mode. Use the **no** form of the command to disable the function.

logging file flash: *filename [max-file-size] [level]*

no logging file

Parameter Description

Parameter	Description
filename	Name of the log file of txt type
max-file-size	Maximal size of the log file in the range from 128 K to 6 M bytes, the default value is 128K bytes.
level	The severity of logs recorded in the log files. The name of the severity or the numeral can be used. By default, the severity of logs recorded in the FLASH is 6. For the details of log severity, see Table-1.

Defaults Logs cannot be recorded in the extended FLASH.

Command Mode Global configuration mode

Usage Guidenes If no **Syslog Server** is specified or it is not desired to transfer logs on the network due to the consideration of security purpose, it is possible to save the logs directly in extended flash.
The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.


Caution You must purchase an additional extended FLASH to record logs on it. If there is no extended FLASH, the **logging file flash** command will automatically be hidden, not allowing you to configure it.

Configuration The following example records the logs in the extended flash, with the name **trace.txt**, file size 128 K

Examples and log severity 6.

```
Ruijie(config)# logging file flash:trace
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Shows the log messages and related log configuration parameters in the buffer.
more flash	Views the logs in the extended flash.

Platform Description None

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 prohibit printing log messages on the VTY window.

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 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	Shows the log messages and related log configuration parameters in the buffer.

Platform Description	None

logging on

Use this command globally to allow logs to be displayed on different devices. Use the **no** form of this command to disable the 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 extended FLASH and 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	Sends logs to the Syslog server.
logging file flash:	Records logs on the extended 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	None

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. The **no** form of this command disables log rate limit 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	Views log information about modules of the system.
show logging	Views basic configuration of log modules and log information in the buffer.

Platform Description None

logging server

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

Usage Guide This command specifies a Syslog server to receive the logs of the device. Users are allowed to configure up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

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	Views 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 None

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 remove the settings.

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 None

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	Sends the logs to the Syslog server.

Platform Description None

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 remove the settings.

logging source interface *interface-type interface-number*

no logging source interface

Parameter Description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.

Defaults None

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	Sends logs to the Syslog server.

Platform Description None

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 disable this function.

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	Views the configuration.

Platform Description None

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 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	Show the log messages and related log configuration parameters in the buffer.

Platform Description

None

service sequence-numbers

Use this command to attach serial numbers into the logs in global configuration mode. Use the **no** form of the command to remove the serial numbers in the logs.

service sequence-numbers

no service sequence-numbers

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No serial number is carried 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	**None**

service sysname

Use this command to attach system name to logs in global configuration mode. Use the **no** form of the command to remove the system name from the logs.

service sysname

no service sysname

Parameter Description

Parameter	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

Related Commands

Command	Function
show logging	Shows basic configuration of log modules and log information in the buffer.

Platform Description	None

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 timestamps of logs to the default values.

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 None

terminal monitor

Use this command to show logs on the current VTY window. Use the **no** form of this command to disable the function.

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 None

show logging

Use this command to show 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 None

Command Mode Privileged EXEC mode

Usage Guide None

Configuration Examples The following command shows 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

None

show logging count

Use this command to show 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 None

Command Mode Privileged 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 is the execution 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	Shows basic configuration of log modules and log information in the buffer.
clear logging	Clears the logs in the buffer.

Platform Description None

Device Fault Management Commands

show environment alarms

Use this command to show information about alarm handling, for example, fans check in case of high temperatures.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples Example 1:

```
Ruijie# show environment alarms
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show environment [all]

Use this command to show all device status in the current fault management.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples Example 1:

```
Ruijie# show environment
Or
Ruijie# show environment all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show environment fans

Use this command to show the operating status of one or multiple fans.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged user mode

Usage Guide Run this command to show the operating status of one or multiple fans, including:
Number of fans and whether they are working normally.
Currently, capacity check of fans is not supported.

Configuration Examples Example 1:

```
Ruijie# show environment fans
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show environment hardware

Use this command to show the hardware status.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to show the current hardware status , including CPU name and speed.

Configuration Examples Example 1：

```
Ruijie# show environment hardware
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show environment powers

Use this command to show the status of one or multiple power supplies.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to show the status of the current power, including:
Rated operating voltage, number of power supplies, and whether each power is working normally.
Currently, operating voltage and thresholds detections are not supported.

Configuration Examples Example 1：

```
Ruijie# show environment power-supply
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show environment temperature

Use this command to show the current environment temperature.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to show the current environment temperature, that is the temperature inside the cabinet.
Currently, inlet temperature check is not supported.

Configuration Examples Example 1：

```
Ruijie# show environment temperature
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

SNMP Commands

clear snmp locked-ip

Use this command to clear the source IP table that is locked after SNMP consecutive authentications fail.

snmp locked-ip

clear snmp locked-ip { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }

Parameter Description

Parameter	Description
ipv4 *ipv4-address*	Clears a specified source IPv4 address.
ipv6 *ipv6-address*	Clears a specified source IPv6 address.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide This command is used to clear the source IP that is locked after SNMP consecutive authentications fail. It can be used to clear either the whole source IP address table or a specified source IP address. After the source IP address is cleared, SNMP packets from this source IP address can try authentication again.

Configuration Examples The following example shows how to clear a source IP table that is locked after SNMP consecutive authentications fail.

```
Ruijie(config)# clear snmp locked-ip
```

Related Commands

Command	Description
snmp-server authentication attempt	Limits the times of failed SNMP consecutive authentications and specifies the solution after consecutive authentications fail.

Platform Description N/A

no snmp-server

Use this command to disable the SNMP agent function in global configuration mode.

no snmp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults The SNMP agent function is disabled.

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 service.

```
Ruijie(config)# no snmp-server
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

snmp-server authentication attempt

Use this command to limit the times of failed SNMP consecutive authentications and specify the solution after consecutive authentications fail. Use the **no** form of this command to clear restrictions on the limit and the solution.

snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

no snmp-server authentication attempt

Parameter Description

Parameter	Description
times	The limit of failed SNMP authentications within the range from 1 to 10.
exceed	The solution that is taken after the number of failed SNMP authentications exceeds the limit.
lock	The source IP address is prevented from authentication permanently. It is blacklisted unless relieved by the administrator manually.
lock-time *minutes*	The source IP address is prevented from authentication for a while and then allowed to be authenticated again. *minutes* refers to the period when the source IP address is prevented, within the range from 1 to 65535 minutes.

unlock	The failed authentication user is not restricted. Instead, the user is allowed to login again.

Defaults The limit of failed SNMP consecutive authentications is 3. The solution after consecutive authentications fail is **unlock** (allows the IP address to try access authentication again).

Command mode Global configuration mode

Usage Guide This command is used to blacklist the source IP after SNMP authentications fail. When the failed times exceed the limit, the system will restrict the access authentication according to the solutions configured by the device:

- The source IP address that is prevented from access authentications permanently cannot try access authentication again unless it is relieved by the administrator manually.
- The source IP address that is prevented from access authentications for a while can try access authentication again when the **lock-time** times out or it is relieved by the administrator manually.
- When you try access authentication again, the non-restricted source IP address will pass it as long as you use correct community (for SNMPv1and SNMPv2c) or username (for SNMPv3).

Configuration Examples The following example shows how to set the limit of failed SNMP consecutive authentications to 4 and the **lock-time** to 30 minutes.

```
Ruijie(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

Related Commands

Command	Description
clear snmp locked-ip	Clears the source IP address table that is locked after SNMP consecutive authentications fail.

Platform Description N/A

snmp-server chassis-id

Use this command to specify the SNMP system serial number in global configuration mode. Use the **no** form of this command to restore it to the initial value.

snmp-server chassis-id *text*

no snmp-server chassis-id

Parameter Description

Parameter	Description
text	Text of the system serial number, digits or characters.

Defaults The default serial number is 60FF60.

Command Mode Global configuration mode

Usage Guide The SNMP system serial number is generally the serial number of the machine to facilitate the device identification. The serial number can be viewed by the **show snmp** command.

Configuration Examples The following example specifies the SNMP system serial number as 123456:

```
Ruijie(config)# snmp-server chassis-id 123456
```

Related Commands

Command	Description
show snmp	Shows the SNMP statistics.

Platform Description N/A

snmp-server community

Use this command to specify the SNMP community access string in global configuration mode. Use the **no** form of this command to cancel the specified SNMP community access string.

snmp-server community *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [**ipv6** *ipv6-aclname*] [*aclnum*] [*aclname*]

no snmp-server community *string*

Parameter Description

Parameter	Description
string	Community string, which is equivalent to the communication password between the NMS and the SNMP agent
view-name	Name of the view used for view-based management
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	Serial number of the ACL, which is associated with a specified access list, specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which is associated with a specified access list, specifies the IPV4 address range of the NMS that are permitted to access the MIB.
ipv6-aclname	Name of the IPv6 ACL, which is associated with a specified access list, specifies the IPv6 address range of the NMS that are permitted to access the MIB
ipaddr	**Specifies** IP address of the NMS accessing the MIB, which is

	associated with NMS addresses.

Defaults All communities are read only by default.

Command Mode Global configuration mode

Usage Guide This command is the first important command to enable the SNMP agent function. It specifies the community attribute, range of the NMSs that can access the MIB, and more.
To disable the SNMP agent function, run the **no snmp-server** command.

Configuration Examples The following example restricts the access to the MIB using the access list, which allows only the NMS of the IP address 192.168.12.1 to access the MIB.

```
Ruijie(config)# access-list 2 permit 192.168.12.1
Ruijie(config)# access-list 2 deny any
Ruijie(config)# snmp-server community public ro 2
```

Related Commands

Command	Description
access-list	Defines the access list.

Platform Description N/A

snmp-server contact

Use this command to specify the SNMP system contact in global configuration mode. Use the **no** form of this command to delete the system contact.

snmp-server contact *text*

no snmp-server contact

Parameter Description

Parameter	Description
text	Character string describing the system contact.

Defaults N/A

Command Mode Global configuration mode

Usage Guide **N/A**

Configuration Examples The following example specifies the SNMP system contract to i-net800@i-net.com.cn:

```
Ruijie(config)# snmp-server contact i-net800@i-net.com.cn
```

Related Commands

Command	Description
show snmp-server	Checks the SNMP information.
no snmp-server	Disables the SNMP agent function.

Platform Description N/A

snmp-server enable traps

Use this command to enable the SNMP server to actively send the SNMP Trap massage to NMS when some emergent and important events occur in global configuration mode. Use the **no** form of this command to disable the SNMP server to actively send the SNMP Trap massage to NMS.

snmp-server enable traps [snmp]

no snmp-server enable traps

Parameter Description

Parameter	Description
snmp	Enables the trap notification of SNMP events.

Defaults The Trap notification is disabled by default.

Command Mode Global configuration mode

Usage Guide This command must work with the global configuration command **snmp-server host** to send the SNMP Trap message.

Configuration Examples The following example enables the SNMP server to actively 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

Platform Description N/A

snmp-server group

Use this command to set the **SNMP** user group in the global configuration mode**.** The **no** form of this command is used to remove the user 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 SNMP Version.
auth	Authenticate the messages transmitted by the user group without encryption. This applies to only SNMPv3.
noauth	Neither authenticate nor encrypt the messages transmitted by the user group. This applies only to SNMPv3.
priv	Authenticate and encrypt the messages transmitted by the user group. This applies only to SNMPv3.
readview	Associate with a read-only view.
writeview	Associate with a read-write view.
aclnum	Serial number of the ACL, which is associated with a specified access list, specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which is associated with a specified access list, specifies the IPV4 address range of the NMS that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 ACL, which is associated with a specified access list, specifies the IPv6 address range of the NMS that are permitted to access the MIB

Defaults No user group is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets a user group.

```
Ruijie(config)# snmp-server group mib2user v3 priv read mib2
```

Related Commands

Command	Description
show snmp group	Shows the SNMP user group configuration.

Platform Description	N/A

snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message in global configuration mode. Use the **no** form of this command to remove the specified SNMP host.

snmp-server host { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]

no snmp-server host { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*]

Parameter Description

Parameter	Description
host-addr	SNMP host address
ipv6-addr	SNMP host address(ipv6)
vrfname	Sets the name of vrf forwarding table
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 sent actively, such as **snmp**.

Defaults

No SNMP host is specified by default.
If no type of the SNMP trap message is specified, all types of the SNMP trap message are included.

Command Mode

Global configuration mode

Usage Guide

This command must work with the **snmp-server enable traps** command in global configuration mode to actively send the SNMP trap messages to NMS.
You can configure multiple SNMP hosts to receive the SNMP Trap messages. One host can use different combinations of the types of the SNMP trap message, different ports and different VRF forwarding tables, but the last configuration for the same host (same port, same VRF configuration) will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages have to 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 to send the SNMP trap message.

Platform Description	N/A

snmp-server location

Use this command to set the SNMP system location information in global configuration mode. Use the **no** form of this command to remove the specified SNMP system location information.

snmp-server location *text*

no snmp-server location

Parameter Description

Parameter	Description
text	Character string describing the system information

Defaults	Null
Command Mode	Global configuration mode
Usage Guide	N/A
Usage Guide	N/A

Configuration Examples

The following example specifies the system information:

```
Ruijie(config)# snmp-server location start-technology-city 4F of A Buliding
```

Related Commands

Command	Description
snmp-sever contact	Specifies the system contact information.

Platform Description	N/A

snmp-server packetsize

Use this command to specify the maximum size of the SNMP packet in global configuration mode. Use the **no** form of this command to restore it to the default value.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter Description

Parameter	Description
byte-count	Packet size in the range from 484 to 17876 bytes

Defaults 1472 bytes.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example specifies the maximum SNMP packet size as 1,492 bytes:

```
Ruijie(config)# snmp-server packetsize 1492
```

Related Commands

Command	Description
snmp-server queue-length	Specifies the length of the SNMP trap message queue.

Platform Description N/A

snmp-server queue-length

Use this command to specify the length of the SNMP trap message queue in global configuration mode.

snmp-server queue-length *length*

Parameter Description

Parameter	Description
length	Queue length in the range from 1 to 1000

Defaults 10.

Command Mode Global configuration mode

Usage Guide The SNMP trap message queue is used to store the SNMP trap messages. This command can be used to adjust the size of the SNMP trap message queue to control the speed to sending the SNMP trap messages.
The maximum speed to send messages is 4 messages per second.

Configuration Examples The following example specifies the speed to send the trap message as 4 messages per second:

```
Ruijie(config)# snmp-server queue-length 4
```

Related Commands

Command	Description
snmp-server packetsize	Specifies the maximum size of the SNMP packet.

Platform Description	N/A

snmp-server system-shutdown

Use this command to enable the SNMP system restart notification function in global configuration mode. Use the **no** form of this command to disable the SNMP system notification function.

snmp-server system-shutdown

no snmp-server system-shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults The SNMP system restart notification function disabled by default.

Command Mode Global configuration mode

Usage guidelines This command is used to enable the SNMP system restart notification function. The RGOS sends the SNMP trap messages to the NMS to notify the system restart before the device is reloaded or rebooted.

Configuration Examples The following example enables the SNMP system restart notification function:

```
Ruijie(config)# snmp-server system-shutdown
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

snmp-server trap-source

Use this command to specify the source address of the SNMP trap message in global configuration mode. Use the **no** form of this command to restore it to the default value.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter Description

Parameter	Description
interface	Interface used as the source of the SNMP trap message.

Defaults The IP address of the interface where the NMP message is sent from is used as the source address.

Command Mode Global configuration mode

Usage Guide The IP address of the interface where the NMP message is sent from is just the source address by default. For easy management and identification, this command can be used 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 of the SNMP trap message:

```
Ruijie(config)# snmp-server trap-source fastethernet 0/1
```

Related Commands

Command	Description
snmp-server enable traps	Enables the sending of the SNMP trap message.
snmp-server enable host	Specifies the NMS host.

Platform Description N/A

snmp-server trap-timeout

Use this command to define the retransmission timout time of the SNMP trap message in the global configuration mode. The **no** form of this command is used to restore it to the default value.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter Description

Parameter	Description
seconds	Timeout period (in seconds) in the range from 1 to 1000.

Defaults 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

Command	Description

Commands		
	snmp-server queue-length	Specifies the length of the SNMP trap message queue.
	snmp-server enable host	Specifies the NMS host

Platform Description N/A

snmp-server user

Use this command to set the SNMP user in global configuration mode**.** Use the **no** form of this command to delete the user.

snmp-server user *username groupname* {**v1 | v2 | v3** [**encrypted**] [**auth** {**md5 | sha**} *auth-password*] [**priv des56** *priv-password*]} [**access** {[**ipv6** *ipv6_aclname*][*aclnum* | acl*name*}]]

no snmp-server user *username groupname* {**v1 | v2c | v3** }

Parameter Description

Parameter	Description
username	User name
groupname	Group name of the user.
v1 | v2 | v3	SNMP Version. But only SNMPv3 supports the following security parameters.
encrypted	Input the password in cipher text mode. In cipher text mode, input consecutive HEX alphanumeric 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 only be used by the local SNMP engine on the switch.
auth	Specifies whether to use the authentication.
md5	Enables the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
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	Specifies whether to use the encryption. **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.
aclnum	Serial number of the ACL, which is associated with the specified access list, specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which is associated with the specified access list, specifies the IPV4 address range of the NMS that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 ACL, which is associated with the specified

	access list, specifies the IPv6 address range of the NMS that are permitted to access the MIB.

Defaults No user is set by default.

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	Shows the SNMP user configuration.

Platform Description N/A

snmp-server view

Use this command to set an SNMP view in global configuration mode**.** Use the **no** form of this command to delete the 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	The MIB object associated with the view is an MIB sub tree.
include	Indicates that the sub trees of the MIB object are included in the view.
exclude	Indicates that the sub trees of the MIB object are excluded from the view.

Defaults A default view is set to access all MIB objects by default.

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	Shows the view configuration.

Platform Description

N/A

snmp trap link-status

For this command, refer to the *INTF-CREF.doc*

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Refer to the *INTF-CREF*.doc.

Command Mode

Refer to the *INTF-CREF*.doc.

Usage Guide

Refer to the *INTF-CREF*.doc.

Configuration Examples

Refer to the *INTF-CREF.doc*

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show snmp

Use this comand to show the SNMP status information in privileged EXEC mode.

show snmp [mib | user | view | group | host]

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide
show snmp: Show the SNMP statistics.
show snmp mib: Show the SNMP MIBs supported in the system.
show snmp user: Show the SNMP user information.
show snmp view: Show the SNMP view information.
show snmp group: Show the SNMP user group information.
Show snmp host: show the display information configured by users.

Configuration Examples
The following example shows an SNMP statistics:

```
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 1500)
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 serial number.

Platform Description N/A

CWMP Commands

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

encryption-type: 0

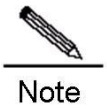
encrypted-password: N/A

Command Mode

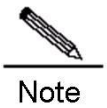
CWMP configuration mode

Usage Guide

Use this command to configure the ACS user password to be authenticated for the CPE to connect to the ACS. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:



The command contains English letters in upper or lower case and numeric characters.



Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples

The following example configures the ACS password to be authenticated for the CPE to connect to the ACS to 123.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Ruijie(config)#cwmp

Ruijie(config-cwmp)#acs password 123

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Platform Description N/A

acs url

Use this command to configure the URL of the ACS to which the CPE will connect.
Use the **no** form of this command to restore the default setting.
acs url *url*
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 formatted as http://host[:port]/path.
- 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	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

acs username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to restore the default setting.

acs username *username*

no acs username

Parameter Description

Parameter	Description
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 terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#acs username admin

Ruijie(config-cwmp)#
```

Related

Command	Description

Commands

show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs password	Configures the ACS password to be authenticated for the CPE to connect to the ACS.

Platform Description N/A

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, in the range from 30 to 10,000 in the unit of seconds

Defaults The default is 60 seconds.

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 terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#no cpe back-up
```

```
Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

cpe back-up

Use this command to enable the CPE backup function.

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

cpe back-up [**delay-time** *seconds*]

no cpe back-up

Parameter Description

Parameter	Description
seconds	Sets the backup delay time (10-600 seconds).

Defaults The default is 30 seconds.

Command Mode CWMP configuration mode

Usage Guide After updrading main programs or configurations, CPE cannot communicate with ACS for wrong configuration delivery. Use this command to recover the previous programs and configurations.

Configuration Examples The following example disables the CPE backup function.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#no cpe back-up

Ruijie(config-cwmp)#
```

Platform Description N/A

cpe inform

Use this command to configure the periodic notification function of the CPE.

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

cpe inform [**interval** *seconds*] [**starttime** *time*]

no cpe inform

Parameter Description

Parameter	Description
seconds	Specifies the periodical notification interval of the CPE in the range from 30 to 3,600 in the unit of seconds.
time	Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.

Defaults The default is 600 seconds.

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the periodic notification function of the CPE.

- If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval.
- If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

Note

The narrower periodical notification interval allows the ACS to track the latest CPE status more accurately. However, narrower periodical notification interval brings about more sessions between the CPE and the ACS, consuming more resources of them. So the user should specify the periodical notification interval of the CPE to a reasonable value according to the network performance and the ACS performance.

Configuration Examples The following example specifies the periodical notification interval of the CPE to 60 seconds.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#cpe inform interval 60

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

cpe password

Use this command to configure the CPE password to be authenticated for the ACS to connect to the CPE. Use the **no** form of this command to cancel the configuration.

cpe password { *password* | *encryption-type encrypted-password* }

no cpe password

Parameter Description

Parameter	Description
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.

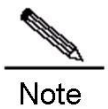
Defaults

encryption-type: 0

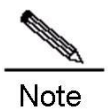
encrypted-password: N/A

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:



Note The command contains English letters in upper or lower case and numeric characters.



Note Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples The following example configures the CPE password to be authenticated for the ACS to connect to the CPE to 123.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#cpe password 123

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Platform Description N/A

cpe url

Use this command to configure the URL of the CPE to which the ACS will connect.
Use the **no** form of this command to restore default setting.
cpe url *url*
no cpe url

Parameter Description

Parameter	Description
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 formatted as http://ip [: port]/ path.
- The URL of the CPE consists of at most 256 characters.

Configuration Examples The following example specifies the URL of the CPE to http://10.10.10.1:7547/acs.

```
Ruijie#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#cpe url http://10.10.10.1:7547/

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

cpe username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS.

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

cpe username *username*

no cpe username

Parameter Description

Parameter	Description
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 terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Ruijie(config)#cwmp

Ruijie(config-cwmp)#cpe username admin

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
cpe password	Configures the CPE password to be authenticated for the ACS to connect to the CPE.

Platform Description N/A

cwmp

Use this command to enable the CWMP function.

Use the **no** form of this command to disable this function.

cwmp

no cwmp

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, this function is enabled.

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable the CWMP function.

Configuration Examples The following example disables the CWMP function.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#no cwmp

Ruijie(config)#
```

Related

Command	Description

Commands

show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

disable download

Use this command to disable the function of downloading main program and configuration files from the ACS. Use the **no** form of this command to restore the default setting.

disable download

no disable download

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the CPE can download main program and configuration files from the ACS.

Command Mode CWMP configuration mode

Usage Guide N/A

Configuration Examples The following example disables the function of downloading main program and configuration files from the ACS.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#disable download

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

disable upload

Use this command to disable the function of uploading configuration and log files to the ACS.

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

disable upload

no disable upload

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the CPE can upload its configuration and log files to the ACS.

Command Mode CWMP configuration mode

Usage Guide Disables the function of uploading configuration and log files to the ACS.

Configuration Examples The following example disables the function of uploading configuration and log file to the ACS.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#disable upload

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

show cwmp configuration

Use this command to display the current configuration of CWMP.

show cwmp configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privilege EXEC mode

Usage Guide

Configuration Examples The following example displays 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 password	ACS password to be authenticated for the CPE to connect to the ACS.
CPE URL	URL of the CPE。
CPE username	CPE username to be authenticated for the ACS to connect to the CPE.

CPE pass ord	CPE password to be authenticated for the ACS to connect to the CPE.
CPE inform status	Status of CPE periodical notification function.
CPE inform interval	CPE periodical notification interval.
CPE wait timeout	Timeout period of CPE sessions.
CPE inform start time	The start time of periodical notification.
CPE download status	Indicates whether to download main program and configuration files from the ACS.
CPE upload status	Indicates whether to upload configuration files and log files to the ACS.
CPE back up status	Indicates whether backup and restoration of the main program and configuration file is enabled.
CPE back up delay time	Delay time of the backup and restoration of the main program and configuration files.

Related Commands

Command	Description
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

show cwmp status

Uses this command to display the running status of CWMP

show cwmp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the running status of CWMP.

```
Ruijie#show cwmp status

CWMP Status                  : enable

Session status               : Close
```

```
Last success session          : Unknown

Last success session time      : Thu Jan  1 00:00:00 1970

Last fail session             : Unknown

Last fail session time         : Thu Jan  1 00:00:00 1970

Session retry times           : 0
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	The running status of CWMP
Session status	The current status of the session between the CPE and the ACS
Last success session	The last success session type
Last success session time	The last success session time
Last fail session	The last failed session type
Last fail session time	The last failed session time
Session retry times	The number of session retransmission attempts

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.

Platform Description N/A

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	Sets the session timeout, in the range from 10 to 600 in the unit of seconds.

Defaults By default, the session timeout period is 30 seconds.

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the session timeout period of the CPE.

The maximum waiting period that the CPE has when the CPE failed to receive the ACS reply.

Configuration Examples The following example configures the session timeout period of the CPE to 50 seconds.

```
Ruijie#config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Ruijie(config)#cwmp

Ruijie(config-cwmp)#timer cpe-timeout 50

Ruijie(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

USB/SD Commands

sd remove

sd remove *device_ID*

Parameter Description

Parameter	Description
device_ID	Device ID. It is contained in the displaying information of the SD device, and can be obtained by the **show sd** command.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Before pulling out the SD device, you need to remove the device using a command to prevent errors occur because the system is using the device. If the device is removed successfully, the system will print a prompt, when you can pull out the device. If the device cannot be pulled out, it indicates that the system is using this SD device, so you have to wait a moment before removing it again.

Configuration Examples The following example removes the SD device mentioned in the example in the previous section.

```
Ruijie# sd remove 1
OK, now you can pull out the device 1.
```

At this moment, the SD card can be plugged out.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show sd

Use this command to show the information about the inserted SD device in the system.

show sd

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 SD device. Otherwise, there is no output.

Configuration Examples The following example shows the information about the SD device:

```
Ruijie# show sd
Device: Mass Storage:
        ID: 1
        URL prefix: sd0
        Disk Partitions:
        SD(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.

Field	Description
URL	Prefix used to access the SD device.
Size	Accessible size of the SD device.
Available size	Available size of the SD device.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show usb

Use this command to show 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.

Configuration Examples The following example shows 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.

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

usb remove

usb remove *device_ID*

Parameter Description

Parameter	Description
device_ID	Device ID. It is contained in the displaying information of the USB device, and can be obtained by the **show usb** command.

Defaults None

Command Mode Privileged EXEC mode

Usage Guide Before pulling out the USB device, you need to remove the device using a command to prevent errors occur because the system is using the device. If the device is removed successfully, the system will print 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 mentioned in the example in the previous section.

```
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

CPU-LOG Commands

cpu-log

Use this command to configure the thresholds for triggering CPU utilization logs manually.

cpu-log log-limit low_num high_num

Parameter Description

Parameter	Description
log-limit	The command descriptor prompting the log limit
low_num	Sets the low threshold for triggering CPU utilization logs.
high_num	Sets the high threshold for triggering CPU utilization logs.

Defaults By default, the high and low thresholds for triggering CPU utilization logs are 100% and 90% respectively.

Command Mode Global configuration mode

Usage Guide Use this command to configure the low and high thresholds for triggering CPU utilization logs manually. When the CPU utilization is higher than the high threshold, a log is sent. If the CPU utilization is continuously higher than the high threshold, the log is sent only once. When the CPU utilization is lower than the low threshold, a log is sent, indicating that the current CPU utilization has decreased. The log is sent only when the CPU utilization changes from a value higher than the high threshold to a value lower than the low threshold.

Configuration Examples The following example sets the low and high thresholds for triggering CPU utilization logs to 70% and 80% respectively.

```
ruijie(config)# cpu-log log-limit 70 80
```

If the CPU utilization is higher than 80%, the following information is displayed:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE_LOG: CPU utilization rate in one minute: 95%. rl_con occupied most CPU utilization rate: 94%.
```

If the CPU utilization is lower than 70%, the following information is displayed:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE_LOG: CPU utilization rate in one minute: 68%. rl_con occupied most CPU utilization rate: 60%.
is ktimer: 60%
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE_LOG: The CPU utilization ratio has been decreased.
```

Related Commands

Command	Description
N/A	N/A

Platform Description	None

show cpu

Use the **show cpu** command to show CPU utilization information in privileged user mode.

show cpu

Parameter Description

Parameter	Description
N/A	N/A

Defaults	None
Command Mode	Privileged user mode
Usage Guide	Use this command to show total system CPU utilization and the CPU utilization of various tasks in the last 5 seconds, 1 minute and 5 minutes respectively.

Configuration Examples

The following example shows the output result of the **show cpu** command.

```
Ruijie# show cpu
 =====================================
    CPU Using Rate Information
CPU utilization in five seconds: 25%
CPU utilization in one minute  : 20%
CPU utilization in five minutes: 10%
  NO   5Sec   1Min   5Min   Process
  0     0%     0%     0%    LISR INT
  1     7%     2%     1%    HISR INT
  2     0%     0%     0%    ktimer
  3     0%     0%     0%    atimer
  4     0%     0%     0%    printk_task
  5     0%     0%     0%    waitqueue_process
  6     0%     0%     0%    tasklet_task
  7     0%     0%     0%    kevents
  8     0%     0%     0%    snmpd
  9     0%     0%     0%    snmp_trapd
 10     0%     0%     0%    mtdblock
 11     0%     0%     0%    gc_task
 12     0%     0%     0%    Context
 13     0%     0%     0%    kswapd
 14     0%     0%     0%    bdflush
 15     0%     0%     0%    kupdate
```

```
16    0%    3%    1%    ll_mt
17    0%    0%    0%    ll main process
18    0%    0%    0%    bridge_relay
19    0%    0%    0%    d1x_task
20    0%    0%    0%    secu_policy_task
21    0%    0%    0%    dhcpa_task
22    0%    0%    0%    dhcpsnp_task
23    0%    0%    0%    igmp_snp
24    0%    0%    0%    mstp_event
25    0%    0%    0%    GVRP_EVENT
26    0%    0%    0%    rldp_task
27    0%    2%    1%    rerp_task
28    0%    0%    0%    reup_event_handler
29    0%    0%    0%    tpp_task
30    0%    0%    0%    ip6timer
31    0%    0%    0%    rtadvd
32    0%    0%    0%    tnet6
33    2%    0%    0%    tnet
34    0%    0%    0%    Tarptime
35    0%    0%    0%    gra_arp
36    0%    0%    0%    Ttcptimer
37    8%    1%    0%    ef_res
38    0%    0%    0%    ef_rcv_msg
39    0%    0%    0%    ef_inconsistent_daemon
40    0%    0%    0%    ip6_tunnel_rcv_pkt
41    0%    0%    0%    res6t
42    0%    0%    0%    tunrt6
43    0%    0%    0%    ef6_rcv_msg
44    0%    0%    0%    ef6_inconsistent_daemon
45    0%    0%    0%    imid
46    0%    0%    0%    nsmd
47    0%    0%    0%    ripd
48    0%    0%    0%    ripngd
49    0%    0%    0%    ospfd
50    0%    0%    0%    ospf6d
51    0%    0%    0%    bgpd
52    0%    0%    0%    pimd
53    0%    0%    0%    pim6d
54    0%    0%    0%    pdmd
55    0%    0%    0%    dvmrpd
56    0%    0%    0%    vty_connect
57    0%    0%    0%    aaa_task
58    0%    0%    0%    Tlogtrap
59    0%    0%    0%    dhcp6c
```

```
 60    0%    0%    0%   sntp_recv_task
 61    0%    0%    0%   ntp_task
 62    0%    0%    0%   sla_deamon
 63    0%    3%    1%   track_daemon
 64    0%    0%    0%   pbr_guard
 65    0%    0%    0%   vrrpd
 66    0%    0%    0%   psnpd
 67    0%    0%    0%   igsnpd
 68    0%    0%    0%   coa_recv
 69    0%    0%    0%   co_oper
 70    0%    0%    0%   co_mac
 71    0%    0%    0%   radius_task
 72    0%    0%    0%   tac+_acct_task
 73    0%    0%    0%   tac+_task
 74    0%    0%    0%   dhcpd_task
 75    0%    0%    0%   dhcps_task
 76    0%    0%    0%   dhcpping_task
 77    0%    0%    0%   dhcpc_task
 78    0%    0%    0%   uart_debug_file_task
 79    0%    0%    0%   ssp_init_task
 80    0%    0%    0%   rl_listen
 81    0%    0%    0%   ikl_msg_operate_thread
 82    0%    0%    0%   bcmDPC
 83    0%    0%    0%   bcmL2X.0
 84    3%    3%    3%   bcmL2X.0
 85    0%    0%    0%   bcmCNTR.0
 86    0%    0%    0%   bcmTX
 87    0%    0%    0%   bcmXGS3AsyncTX
 88    0%    2%    1%   bcmLINK.0
 89    0%    0%    0%   bcmRX
 90    0%    0%    0%   mngpkt_rcv_thread
 91    0%    0%    0%   mngpkt_recycle_thread
 92    0%    0%    0%   stack_task
 93    0%    0%    0%   stack_disc_task
 94    0%    0%    0%   redun_sync_task
 95    0%    0%    0%   conf_dispatch_task
 96    0%    0%    0%   devprob_task
 97    0%    0%    0%   rdp_snd_thread
 98    0%    0%    0%   rdp_rcv_thread
 99    0%    0%    0%   rdp_slot_change_thread
100    4%    2%    1%   datapkt_rcv_thread
101    0%    0%    0%   keepalive_link_notify
102    0%    0%    0%   rerp_msg_recv_thread
103    0%    0%    0%   ip_scan_guard_task
```

```
104     0%     0%     0%    ssp_ipmc_hit_task
105     0%     0%     0%    ssp_ipmc_trap_task
106     0%     0%     0%    hw_err_snd_task
107     0%     0%     0%    rerp_packet_send_task
108     0%     0%     0%    idle_vlan_proc_thread
109     0%     0%     0%    cmic_pause_detect
110     1%     1%     1%    stat_get_and_send
111     0%     1%     0%    rl_con
112    75%    80%    90%     idle
```

In the list above, the first 3 lines indicate the system CPU utilization in the last 5 seconds, 1 minute and 5 minutes respectively, including the CPU utilization of LISRs, HISRs and tasks, followed by the CPU utilization of various processes. The parameters in the columns are described as follows:

Field	Description
No	Sequence number
5Sec	CPU utilization of the task in the last 5 seconds
1Min	CPU utilization of the task in the last 1 minute
5Min	CPU utilization of the task in the last 5 minutes

The first 2 lines in the list above indicate the CPU utilization of all LISRs and HISRs. All lines starting from the 3rd line indicate the CPU utilization of specific tasks. The last line indicates the CPU utilization of idle tasks, which is the same as **System Idle Porcess** in the Windows operating system. In the example above, the CPU utilization of idle tasks within the last 5 seconds is 75%, indicating that 75% of the CPU resources are available.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Memory Commands

memory-lack exit-policy

Use this command to set the exit-policy of the upper route protocol when the memory reaches the lower threshold. The upper route protocol includes BGP,OSPF,RIP,PIM-SM.

memory-lack exit-policy {**bgp** | **ospf** | **pim-sm** | **rip**}

no memory-lack exit-policy

Parameter Description

Parameter	Description
bgp|ospf|pim-sm|rip	Specifies the route protocol: BGP, OSPF, PIM or RIP.
no	Restores the default setting.

Defaults Exit the route protocol that occupies the largest memory.

Command Mode Global configuration mode

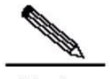
Usage Guide

When the memory size reaches the lower threshold, which can be viewed by using the **show memory** command, a route protocol will be disabled to release the memory to ensure operation of other protocols.

You will know that what route protocols support the major services in the network. When the memory lacks, you can disable the least important protocol to ensure the operation of major services.

For example, in a user network, BGP route is irrelevant to the network core services. You can configure the BGP exit-policy when the memory lacks.

Specifying the disabled route protocol to take precedence to exit the policy can not help the system obtain enough memory resources.


Note

The exit-policy is used to protect important network services to some degree. All route protocols will exit if more memory resources are exhausted. 2 minutes after existing the protocol, the route protocol will restart.

Configuration Examples This example enables the BGP to exit from the policy prior to other protocols:

```
Ruijie(config)# memory-lack exit-policy bgp
```

Related Commands

Command	Description
show memory	Shows the current memory usage information.

Platform Description	N/A

show memory

Use this command to show the current memory usage information.

show memory

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

Defaults	N/A
Command Mode	Privileged EXEC mode

Usage Guide

Use this command to view the current system memory state and usage information, including the system physical memory amount, the number of free pages in the current system, the free memory statistics.

The following example shows the output of the **show cpu** command:

```
Ruijie#show memory
System Memory Statistic:
  Free pages: 1079
  watermarks : min 379, lower 758, low 1137, high 1516
  System Total Memory : 128MB, Current Free Memory : 5283KB
Used Rate : 96%
```

The above information includes:

1) Free pages: the memory size of one free page is about 4k;
2) Watermarks (see the following table)

Configuration Examples

Parameter	**Description**
min	Memory resources are extremely insufficient. It can only support the kernel running. All application modules fails to run if the minimum watermark has been reached.
lower	Memory resources are severely insufficient. One route protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the **memory-lack exit-policy** command.
low	Memory resources are insufficient. The route protocol will be in OVERFLOW state if the low

	watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	There is plenty of memory resources. Each route protocol attempts to restore the state from OVERFLOW to normal.

3) System total memory, current free memory and used rate.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show memory protocols

Use this command to display the usage of the memory for the route protocols.

show memory protocols

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode

Use this command to display the usage of the memory for the route protocols.

Usage Guide

Note Different switches and versions support different route protocols. Main route protocols include BGP, OSPF, RIP, LDP, PIM and ISIS.

This example shows the result of the command show memory protocols:

Configuration Examples

```
Ruijie(config)# show memory protocols
=====================================================
protocol      |memory(byte)
BGP            102000000
OSPF            24000000
RIP             10000000
PIM             50000000
LDP             20000000
```

```
Total          206000000
```

Related Commands	Command	Description
	show memory	Shows the current memory usage information.

Platform Description

N/A

Debugging Improvement Commands

show tech-support

Use this command to collect information of modules using the one-key mode.

show tech-support {*module-name*}

Description

Parameter	Description
module-name	Indicates the module name.

Default Configuration

The debugging information of all modules is collected.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example collects the debugging information of all modules.

```
Ruijie# show tech-support
Save in file? [yes]
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

FPM Commands

clear ip fpm counters

Use this command to clear IPv4 packet statistics of the flow platform.

clear ip fpm counters

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

Note This command is supported on RGOS 10.4(3) or later.

Configuration Examples The following example clears IPv4 statistics of the flow platform.

```
Ruijie# clear ip fpm counters
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear ip fpm flows

Use this command to clear the IPv4 flow table of the flow platform.

clear ip fpm flows

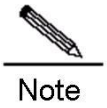
Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide



Note

This command is supported on RGOS 10.4(3) or later. Clearing the flow table is an asynchronous operation, therefore it takes several seconds to finish clearing after this command is run.

Configuration Examples The following example clears the IPv4 flow table of the flow platform.

```
Ruijie# clear ip fpm flows
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear ipv6 fpm flows

Use this command to clear the IPv6 flow table of the flow platform.

clear ipv6 fpm flows

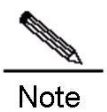
Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide



Note

This command is supported on RGOS 10.4(3b13) or later. Clearing the flow table is an asynchronous operation, therefore it takes several seconds to finish clearing after the command is run.

Configuration Examples The following example clears the IPv6 flow table of the flow platform.

```
Ruijie# clear ipv6 fpm flows
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

clear ipv6 fpm statistics

Use this command to clear IPv6 statistics of the flow platform

clear ipv6 fpm statistics

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

This command is supported on RGOS 10.4(3b13) or later.

Configuration Examples The following example clears IPv6 statistics of the flow platform

```
Ruijie# clear ipv6 fpm statistics
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ip fpm flow alert interval

Use this command to configure the IPv4 flow overflow alarm interval of the flow platform.

ip fpm flow alert interval *seconds*

no ip fpm flow alert interval

default ip fpm flow alert interval

Parameter Description	Parameter	Description

seconds	The IPv4 flow overflow alarm interval. The unit is second.

Defaults The IPv4 flow overflow alarm interval is 5 seconds by default.

Command mode Global configuration mode

Usage Guide

Note This command is supported on RGOS 10.4(3b13) or later.

Configuration Examples The following example configures the IPv4 flow overflow alarm interval of the flow platform.

```
Ruijie# configure terminal
Ruijie(config)# ip fpm flow alert interval 120
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip fpm flow alert threshold

Use this command to configure the IPv4 flow overflow alarm threshold of the flow platform.

ip fpm flow alert threshold *percent-value*

no ip fpm flow alert threshold

default ip fpm flow alert threshold

Parameter Description

Parameter	Description
percent-value	Overflow alarm threshold (the proportion in the total IPv4 flows)

Defaults The IPv4 flow overflow alarm threshold of the flow platform is 95% by default.

Command mode Global configuration mode

Usage Guide

Note This command is supported on RGOS 10.4(3b13) or later.

Configuration The following example configures the IPv4 flow overflow alarm threshold of the flow platform.

Examples

```
Ruijie# configure terminal
Ruijie(config)# ip fpm flow alert threshold 80
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip fpm flow max-entries

Use this command to configure the maximum number of flow entries in the IPv4 flow table.
ip fpm flow alert max-entries *flow-number*
no ip fpm flow alert max-entries
default ip fpm flow alert max-entries

Parameter Description

Parameter	Description
flow-number	Configures the maximum number of IPv4 flow entries.

Defaults The IPv4 flow table contains 180,223 flow entries by default.

Command mode Global configuration mode

Usage Guide


Note

This command is supported on RGOS 10.4(3b13) or later. The configurable total number of flow entries is restricted by the number of IPv4 and IPv6 flow entries. If you want increase the number of IPv4 flow entries, you need to decrease the number of IPv6 flow entries first.


Caution

Altering the number of flow entries may clear the existing flows and suspends data from being forwarded.

Configuration Examples The following example configures the maximum number of flow entries in the IPv4 flow table.

```
Ruijie# configure terminal
Ruijie(config)# ip fpm flow max-entries 120000
FPM subsystem is reinitializing...
Ruijie(config)#*Oct  6 17:35:21: %FPM-5-RESTARTED: The device IPv4 flow
max-entries changed.
```

Related Commands

Command	Description
ipv6 fpm flow max-entries *flow-number*	Configures the maximum number of IPv6 flow entries.

Platform Description N/A

ip fpm frq

Use this command to configure the number of concurrent IPv4 fragment reassembly queues.

ip fpm frq *queue-number*

no ip fpm frq

default ip fpm frq

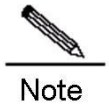
Parameter Description

Parameter	Description
queue-number	Configures the number of concurrent IPv4 fragment reassembly queues supported on the device.

Defaults The number of concurrent IPv4 fragment reassembly queues is 1,024 by default.

Command mode Global configuration mode

Usage Guide



This command is supported on RGOS 10.4(3b13) or later.

Altering the number of concurrent IPv4 fragment reassembly queues clears the existing fragment reassembly queues and suspends data from being forwarded.

Configuration Examples The following example configures the number of concurrent IPv4 fragment reassembly queues.

```
Ruijie# configure terminal
Ruijie(config)# ip fpm frq 4096
fragment reassemble component initializing..
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip fpm session filter

Use this command to protect the IPv4 flow table against attacks.

ip fpm session filter *acl-number*

no ip fpm session filter

default ip fpm session filter

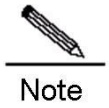
Parameter Description

Parameter	Description
acl-number	Configures the ID of the ACL used to protect the IPv4 flow table against attacks.

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide



This command is supported on RGOS 10.4(3b13) or later. After this command is configured, only sessions allowed by the *acl-number* parameter establish flows.

Configuration Examples The following example protects the IPv4 flow table against attacks.

```
Ruijie# configure terminal
Ruijie(config)# ip access-list standard 1
Ruijie (config-std-nacl)# permit 192.168.50.0 0.0.0.255
Ruijie (config-std-nacl)# deny any
Ruijie (config-std-nacl)# exit
Ruijie(config)# ip fpm session filter 1
```

Related Commands

Command	Description
ip access-list	Configures an ACL

Platform Description N/A

ipv6 fpm flow alert interval

Use this command to configure the IPv6 flow overflow alarm interval of the flow platform.

ipv6 fpm flow alert interval *seconds*
no ipv6 fpm flow alert interval
default ipv6 fpm flow alert interval

Parameter Description

Parameter	Description
seconds	The IPv6 flow overflow alarm interval, with second as the unit.

Defaults The IPv4 flow overflow alarm interval is 5 seconds by default.

Command mode Global configuration mode

Usage Guide


Note This command is supported on RGOS 10.4(3b13) or later.

Configuration Examples The following example configures the IPv6 flow overflow alarm interval of the flow platform.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 fpm flow alert interval 120
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 fpm flow alert threshold

Use this command to configure the IPv6 flow overflow alarm threshold of the flow platform.
ipv6 fpm flow alert threshold *percent-value*
no ipv6 fpm flow alert threshold
default ipv6 fpm flow alert threshold

Parameter Description

Parameter	Parameter
percent-value	Overflow alarm threshold (the proportion in the total IPv6 flows)

Defaults The IPv6 flow overflow alarm threshold of the flow platform is 95% by default.

Command mode Global configuration mode

Usage Guide


Note

This command is supported on RGOS 10.4(3b13) or later.

Configuration Examples

The following example configures the IPv6 flow overflow alarm threshold of the flow platform.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 fpm flow alert threshold 80
```

Related Commands

Command	Command
N/A	N/A

Platform Description

N/A

ipv6 fpm flow max-entries

Use this command to configure the maximum number of flow entries in the IPv6 flow table.

ipv6 fpm flow alert max-entries *flow-number*

no ipv6 fpm flow alert max-entries

default ipv6 fpm flow alert max-entries

Parameter Description

Parameter	Parameter
flow-number	Configures the maximum number of IPv6 flow entries.

Defaults

The IPv6 flow table contains 81,920 flow entries by default.

Command mode

Global configuration mode

Usage Guide


Note

This command is supported on RGOS 10.4(3b13) or later. The configurable total number of flow entries is restricted by the number of IPv4 and IPv6 flow entries. If you want increase the number of IPv6 flow entries, you need to decrease the number of IPv4 flow entries first.


Caution

Altering the number of flow entries requires the existing flows to be cleared and suspends data from being forwarded.

Configuration Examples The following example configures the maximum number of flow entries in the IPv6 flow table.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 fpm flow max-entries 70000
FPM subsystem is reinitializing...
Ruijie(config)#*Oct  6 17:35:21: %FPM-5-RESTARTED: The device IPv6 flow max-entries changed.
```

Related Commands

Command	Command
Ip fpm flow max-entries *flow-number*	Configures the maximum number of IPv4 flow entries.

Platform Description N/A

ipv6 fpm frq

Use this command to configure the number of concurrent IPv6 fragment reassembly queues.

ipv6 fpm frq *queue-number*

no ipv6 fpm frq

default ipv6 fpm frq

Parameter Description

Parameter	Description
queue-number	Configures the number of concurrent IPv6 fragment reassembly queues supported on the device.

Defaults The number of concurrent IPv6 fragment reassembly queues is 1,024 by default.

Command mode Global configuration mode

Usage Guide

This command is supported on RGOS 10.4(3b13) or later.

Altering the number of concurrent IPv6 fragment reassembly queues clears the existing fragment reassembly queues and suspends data from being forwarded.

Configuration Examples The following example configures the number of concurrent IPv6 fragment reassembly queues.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 fpm frq 4096
```

```
fragment reassemble component initializing...
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 fpm session filter

Use this command to protect the IPv6 flow table against attacks.

ipv6 fpm session filter *acl-name*

no ipv6 fpm session filter

default ipv6 fpm session filter

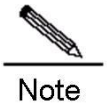
Parameter Description

Parameter	Description
acl-number	Configures the ID of the IPv6 ACL used to protect the IPv6 flow table against attacks.

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide


Note

This command is supported on RGOS 10.4(3b13) or later. After this command is configured, only sessions allowed by the *acl-number* parameter establish flows.

Configuration Examples The following example protects the IPv6 flow table against attacks.

```
Ruijie# configure terminal
Ruijie(config)# ipv access-list antivirus
Ruijie (config-ipv6-acl)# permit ipv6 2001::/64 any
Ruijie (config-ipv6-acl)# permit icmp 2001::/64 any
Ruijie (config-ipv6-acl)# exit
Ruijie(config)# ipv6 fpm session filter antivirus
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL

Platform Description N/A

show ip fpm counters

Use this command to displays IPv4 packet counters of the flow platform.

show ip fpm counters

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

Note This command is supported on RGOS 10.4(3) or later.

Configuration Examples The following command displays IPv4 packet counters of the flow platform.

```
Ruijie# show ip fpm counters
Count     Reason
0         Non-IPv4 packet
0         Bad IPv4 header length
0         Bad IPv4 total length
0         Bad IPv4 checksum
0         Illegal IPv4 address
0         Invalid IPv4 fragment
0         Ipv4 defragment overmuch
0         Ipv4 defragment oversize
0         IPv4 defragment timeout
0         IPv4 defragment out of buffer
0         IPv4 defragment out of context
0         Ipv4 defragment
0         Valid Ipv4 fragment
0         Illegal TCP flags
0         Illegal ICMP message type
0         Flow table overflow
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

show ip fpm flows

Use this command to display the IPv4 flow table.

show ip fpm flows [**filter** *protocol-number src-ip src-mask dst-ip dst-mask*]

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

This command is supported on RGOS 10.4(3) or later.

This command shows only flow records of local card. You need to log into the line card to view flow records of the line card.

Configuration Examples The following example displays the IPv4 flow table.

```
Ruijie# show ip fpm flows
Pr  SrcAddr                          DstAddr                          SrcPort
DstPort     Vrf       SendBytes  RecvBytes  St
17  192.168.46.12                    255.255.255.255                  1629
2654        0         340        0          1
17  192.168.46.12                    255.255.255.255                  1603
2654        0         340        0          1
17  192.168.52.175                   255.255.255.255                  1114
11111       0         41030      0          1
17  10.0.0.2                         224.0.0.2                        646
646         0         26110      0          1
17  30.0.0.1                         224.0.0.2                        646
646         0         26110      0          1
<end>
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip fpm statistics

Use this command to display IPv4 statistics of the flow platform.

show ip fpm statistics

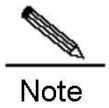
Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide



Note This command is supported on RGOS 10.4(3) or later.

Configuration Examples The following example displays IPv4 statistics of the flow platform.

```
Ruijie# show ip fpm statistics
Flow table capacity: 120000
Flow number: 73
Nat-flow number: 0
User number: 30
Defragment context number: 0
Defragment packet number: 0
Event count: 45
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip fpm users

Use this command to display the number of IPv4 user connections of the flow platform.

show ip fpm users

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

Note This command is supported on RGOS 10.4(3) or later.

Configuration Examples The following example displays the number of IPv4 user connections of the flow platform.

```
Ruijie# show ip fpm users
IP-address       Active-time(s) Active-Conns
192.168.45.206    61            1
192.168.45.90     51            1
192.168.45.249    61            1
192.168.46.12     7246          42
192.168.52.9      9             1
192.168.52.51     79            1
192.168.50.198    6             1
<end>
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 fpm statistics

Use this command to display IPv6 statistics of the flow platform.

show ipv6 fpm statistics

Parameter

Parameter	Parameter

Description

N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

Note This command is supported on RGOS 10.4(3b13) or later.

Configuration Examples The following example displays IPv6 statistics of the flow platform.

```
Ruijie# show ipv6 fpm statistics
Flow capacity: 81920, FRQ capacity: 1024, Flow number: 0
Extend protocol: 1, Extend module: 3, Extend module sn: 3, Event counter: 41
FBF switch: 1, Flow aging switch: 1
FPM restart: 0, FRQ restart: 0

Packet statistics:
  Fragment in: 0, Send icmp_error: 0
Packet exception statistics:
  Precreate: 0, Illegal icmp: 0, Ingress recognize: 0, Egress recognize: 0
  Track state: 0, Egress rflow: 0, flow overflow: 0
  Bad version: 0, Bad payload len: 0, Illegal source address: 0, Illegal
destination address: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 fpm statistics fragment

Use this command to display IPv6 fragment reassembly statistics of the flow platform.

show ipv6 fpm statistics fragment

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

Note This command is supported on RGOS 10.4(3b13) or later.

Configuration Examples The following example displays IPv6 fragment reassembly statistics of the flow platform.

```
Ruijie# show ipv6 fpm statistics fragment
Fragments cache: 0,  Reassemble success: 0,  Fragments disorder: 0, Send
icmp_error: 0
Drop statistics:
  packet error: 0,  invalid fragment: 0,  frag-guard: 0,  queue limit: 0
  jobogram: 0,  reassemble timeout: 0,  fragment oversize: 0,  frq short: 0
  fragment duplicate: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 fpm flows

Use this command to display the IPv6 flow table.

show ipv6 fpm flows [**filter** *protocol-number src-ip dst-ip*]

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

Note This command is supported on RGOS 10.4(3b13) or later.

Configuration Examples The following example displays the IPv6 flow table.

```
Ruijie# show ipv6 fpm flows
Proto  Source Address                  Destionation Address           SrcPort
DstPort   Vrf   State   RxBytes
58     2000::2                          2000::1                          1
33024    0    2      100
      2000::1                          2000::2                          1
32768    0    2      0


58     2000::2                          2000::1                          0
33024    0    2      100
      2000::1                          2000::2                          0
32768    0    2      0
Total number of flow entries: 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Interface Configuration Commands

1. Interface Commands
2. VLAN Commands
3. Aggregate Port Commands
4. RMON Commands
5. SPAN Commands

Interface Commands

bandwidth

Use this command to set the bandwidth parameters of an interface in interface configuration mode. 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 K bytes per second

Defaults When the **bandwidth** command parameter is not set, the **show interface** command is used to display the default value in privileged user mode.

Command Mode Interface configuration mode

Usage Guide The **bandwidth** command does not actually affect the bandwidth of an interface. Instead, it asks the user to tell the system the bandwidth of the interface. Usually, the bandwidth of the Ethernet interface is fixed. On the other hand, you can set the bandwidth properly for the Serial interface and Async interface. The **bandwidth** parameter is only a route parameter without any influence on the real bandwidth of the interface of the physical link.

Configuration Examples The following example sets the bandwidth parameter to 64 Kbps:

```
Ruijie(config-if)# bandwidth 64
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

carrier-delay

Use this command to set the carrier delay of an interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

carrier-delay { *seconds* }

no carrier-delay

Parameter Description

Parameter	Description
seconds	Optional parameter, in the range from 0 to 60 seconds

Defaults The carrier delay is 2 seconds by default.

Command Mode Interface configuration mode

Usage Guide This parameter is 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 this parameter is set to a great value, nearly every transient DCD change is not detected. On the contrary, if the parameter is set to 0, every minor DCD signal change will be detected by the system, resulting in higher instability.

If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route convergence so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is smaller than the time for route convergence, 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 0 to 5 seconds.

```
Ruijie(config)# interface serial 0
Ruijie(coinfig)# carrier-delay 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

channel-group

Use this command to allocate the timeslot of CE1 to the specified channel-group in CE1 working mode. Use the **no** form of this command to remove this setting.

channel-group *channel-group* **timeslots** *timeslot-range*

no channel-group *channel-group*

Parameter Description

Parameter	Description
channel-group	Channel group number on the CE1 interface, in the range from 0 to 30
timeslot-range	Timeslot range, which can be a single timeslot or multiple

	timeslots. Multiple timeslots are not necessarily to be continuous. The range of the timeslot is from 1 to 31.

Defaults No channel group is configured by default.

Command Mode CE1 interface configuration mode

Usage Guide In CE1 working mode, the data frames of the CE1 interface consist of 32 timeslots numbering 0 through 31. Timeslot 0 is used to transmit the frame synchronization signal, and all or some of other timeslots can be grouped into several channel groups. Each channel group is used as an interface, whose logic is the same as the sync serial interface.

Configuration Examples The following example sets timeslots 1-3, 5 and 7-10 of the CE1 interface to channel group 1.

```
Ruijie(config-controller)# channel-group 1 timeslots 1-3,5,7-10
```

Related Commands

Command	Description
Using { **e1** | **ce1** }	Configures the E1 or CE1 working mode of the CE1 interface.

Platform Description N/A

clear controller e1

Use this command to reset the E1 controller.

clear controller e1 *slot/port*

Parameter Description

Parameter	Description
Slot	Number of the slot where the E1 controller to be reset resides
Port	Number of the serial port of the slot where the E1 controller to be reset resides

Defaults N/A

Command Mode Privileged user mode

Usage Guide Usually, you do not need to perform the reset operation.

Configuration Examples The following example resets the E1 controller with the port number of 0 in slot 1/1

```
Ruijie# clear controller e1 1/1/0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

clear counters

Use this command to clear the counter of the communication parameters of an interface in privileged user mode.

clear counters [*interface-type slot-number/interface-numbe*r]

Parameter Description	Parameter	Description
	interface-type	Interface type, for example, **serial**, **async**; see the interface type list.
	slot-number/interface-number	Slot number/port number of an interface type

Defaults N/A

Command Mode Privileged user mode

Usage Guide The statistics on the interface vary with the change of communication. Sometimes, you need to clear it to avoid the interference caused by old ones to reflect the current communication state accordingly.

Configuration Examples The following example clears the counters of serial interface 1/0.

```
Ruijie# clear counters serial 1/0
```

Related Commands	Command	Description
	show interface	Shows the hardware statistics and link communication status of an interface.

Platform Description N/A

clear interface

Use this command to reset the hardware logic of an interface in privileged user mode.

clear interface *interface-type slot-number/interface-number*

Parameter Description

Parameter	Description
interface-type	Interface type, for example, **serial**, **async**; see the interface type list.
Slot-number/interface-number	Slot number/port number of an interface type

Defaults N/A

Command Mode Privileged user mode

Usage Guide Usually, you do not need to reset the hardware logic of an interface.

List of interface types:

Keyword	Interface Type
async	Async serial interface
dialer	Logical dialer interface
Fastethernet	10/100M fast Ethernet interface
Group-async	Dialer group interface
loopback	Loopback interface
Null	Null interface
serial	Sync serial interface

Configuration Examples The following example resets the hardware logic of serial interface 1/0.

```
Ruijie# clear interface serial 1/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear vlan

Use this command to clear VLAN statistics in privileged user mode.

clear vlan {*VLANID* }

Parameter Description

Parameter	Description
VLANID	ID of the VLAN whose statistics are to be cleared, an integer in the

	range from 1 to 4094 The statistics of all the VLANs will be cleared if no VLAN ID is specified.

Defaults N/A

Command Mode Privileged user mode

Usage Guide N/A

Configuration Examples The following example clears the statistics of all VLANs.

```
Ruijie# clear vlan
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clock source

Use this command to set the sync clock source of the CE1 interface. Use the **no** form of this command to restore the default setting.

clock source { **line | internal** }

no clock source

Parameter Description

Parameter	Description
line	Obtains the sync clock source of the CE1 interface from the data receiving line.
internal	Obtains the sync clock source of the CE1 interface internally.

Defaults The sync clock source of the CE1 interface is line by default.

Command Mode CE1 interface configuration mode

Usage Guide When CE1 interfaces are used, one of them offers a sync clock. When two CE1 interfaces are directly connected, one of them offers a sync clock, and the other obtains the sync clock from the data receiving line. When a CE1 interface is connected to a Layer 2 device, usually the Layer 2 device offers a sync clock. However, the CE1 interface on the Layer 3 device obtains a sync clock from the data receiving line.

Configuration Examples The following example sets the internal clock as the sync clock.

```
Ruijie(config-controller)#clock source internal
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

controller e1

Use this command to enter the configuration layer of the specified CE1 controller interface.

controller e1 *slot/port*

Parameter Description

Parameter	Description
slot	Number of the slot where the E1 controller to be set resides
port	Number of the port of the slot where the E1 controller to be set resides

Defaults N/A

Command Mode Global configuration mode

Usage Guide On the global configuration layer, you can use this command to enter the specified CE1 interface configuration mode.

Configuration Examples The following example configures the CE1 interface with the port number of 1 in slot 1/1.

```
Ruijie(config)# controller e1 1/1/1
Ruijie(config-controller)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug vlan

Use this command to turn on the VLAN debugging switch in privileged user mode. Use the **no** form of this command to turn off the VLAN debugging switch.

debug vlan

no debug vlan

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged user mode

Usage Guide N/A

Configuration Examples The following example turns on the VLAN debugging switch.

```
Ruijie# debug vlan
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

description

Use this command to set the description of an interface in interface configuration mode. Use the **no** form of this command to delete the description.

description *string*

no description

Parameter Description

Parameter	Description
string	Description string of the interface

Defaults No interface description is configured by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example shows the description of the interface: "2 Mbit/s bandwidth, connected to Shandong".

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#description ShanDong-Bandwidth2M
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

duplex

Use this command to set the duplex mode of the Ethernet interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

duplex { **full | half | auto** }

no duplex

Parameter Description

Parameter	Description
full	Specifies the full duplex mode for the Ethernet interface.
half	Specifies the half duplex mode for the Ethernet interface.
auto	Specifies the auto mode for the Ethernet interface. The system will automatically configure the interface to work in the full duplex or half duplex mode according to the actual conditions of the hub, Layer 2 device, and network card connected with the interface.

Defaults Auto mode

Command Mode Interface configuration mode

Usage Guide To set the working mode of the network interface, you can also use the **speed** command in addition to the **duplex** command. For details, see the description of the **speed** command.

Configuration Examples The following example sets Fast Ethernet interface 0/0 to work in half duplex mode.

```
Ruijie(config)#interface fastethernet 0/0
Ruijie(config-if)#duplex half
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

encapsulation dot1q

Use this command to encapsulate IEEE 802.1Q on the sub interface in subinterface configuration mode. Use the **no** form of this command to restore the default setting.

encapsulation dot1Q *VLANID*

no encapsulation

Parameter Description	Parameter	Description
	VLANID	ID of the VLAN, in the range from 1 to 4094

Defaults ARPA is encapsulated on the Ethernet interface by default.

Command Mode Sub interface configuration mode

Usage Guide 802.1Q, an IEEE standard protocol, is used to enable communications between Layer 2 and Layer 3 devices with VLAN partition performed.

802.1Q can only be encapsulated on the sub Ethernet interface.

Configuration Examples The following example encapsulates 802.1Q on the sub interface 20 of VLAN 20.

```
Ruijie(config)# interface fastEthernet 0/0.20
Ruijie(config-subif)#encapsulation dot1Q 20
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

framing

Use this command to set the frame check mode of the CE interface. Use the **no** form of this command to restore the default setting.

This command does not work in E1 working mode.

framing { **crc4 | no-crc4** }
no framing

Parameter Description

Parameter	Description
crc4	Enables the CE1 interface to perform crc4 for physical frames.
no-crc4	Disables the CE1 interface to perform crc4 for physical frames.

Defaults The default setting is crc4.

Command Mode CE1 interface configuration mode

Usage Guide The CE1 interface supports the crc4 check for the CE1 physical frames.

Configuration Examples The following example disables crc4 for the physical frames of the CE1 interface.

```
Ruijie(config-controller)# framing no-crc4
```

Related Commands

Command	Description
Using { **e1** | **ce1** }	Configures the E1 or CE1 working mode of the CE1 interface.

Platform Description N/A

hold-queue

Use this command to set the maximum queue length of an interface in interface configuration mode. Use the **no** form of this command to restore the default setting.
hold-queue *length* { **in | out** }
no hold-queue [*length*] { **in | out** }

Parameter Description

Parameter	Description
length	Maximum length of a queue, in the range from 1 to 4096
in	Indicates that the *length* is the maximum length of the input queue of the interface, 75 by default.
out	Indicates that the *length* is the maximum length of the output queue of the interface, 40 by default.

Defaults The maximum queue length of the Ethernet interface is 40, that of the synchronous/asynchronous serial port is 64, and that of the input queue is 75 by default.

Command Mode Interface configuration mode

Usage Guide The input queue length is set in order to prevent too many data packets from being held in the buffer due to excessive network traffic. As a result, the packets beyond the capability of the system will be discarded. Therefore, when you use the **show interface** command, you can see the utilization of the buffer area as follows, Input queue: 0/75/, 0 drops (size/max/drops), which means the current utilization, maximum length, and number of dropped packets respectively.

If the output queues are prioritized, the setting of the output queue length no longer takes effect. In this case, the output queue is determined based on the queue priority policy.

The input/output queue setting varies with bandwidth. For the link interface of the low-speed bandwidth, you are recommended to set a smaller output queue length, guaranteeing that the packet storage rate will not exceed the transmission rate of the link. For the high-speed bandwidth, you are recommended to set a larger output queue length. The link may be too busy to send data sometimes. However, once the link becomes idle, the data in the buffer can be easily sent to prevent frequent packet drop due to insufficient queue length.

Configuration Examples The following example sets the maximum length of the input queue in serial port 1/0 to 256.

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#hold-queue 256 in
```

Related Commands

Command	Description
show interface	Shows the hardware statistics and link communication status of an interface.

Platform Description N/A

interface

Use this command to enter the interface configuration mode in global configuration mode.

interface *type slot-number/interface-number* [.sub-interface-number] [**multipoint** | **point-to-point**]

Parameter Description

Parameter	Description
type	Interface type, including Ethernet, FastEthernet, Loopback, Null, and Dialer
Slot-number/port-number	Interface number composed of the slot number and port number; the slot number indicates the number of the slot where the interface resides (on the motherboard, the slot number of the interface is 0); the port number indicates the number of the interface on a slot.

sub-interface-number	Sub-interface number for frame relay or X.25 only
multipoint	Point-to-multipoint type in the sub-interface
point-to-point	Point-to-point type in the sub-interface

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

Related Commands

Command	Description
show interface	Shows the hardware statistics and link communication status of an interface.

Platform Description N/A

ip address

Use this command to set the IP address of an interface in interface configuration mode. Use the **no** form of this command to delete the IP address.

ip address *ip-address sub-mask* [**secondary**]

no ip address [*ip-address sub-mask* [**secondary**]]

Parameter Description

Parameter	Description
no ip address [*ip*	*address sub*
no ip address [*ip*	*address sub*
no ip address [*ip*	*address sub*

Defaults The interface is not configured with an IP address by default.

Command Mode Interface configuration mode

Usage Guide Unless the IP protocol is not used, every interface must have an IP address, no matter it is a physical or logical interface. The **ip address** command is the most common method.

When you set the IP address, you must follow the IP address configuration rule: it cannot be in the

same network segment as other interfaces and must be different from any IP address of other hosts or Layer 3 devices on the same LAN. Otherwise, the network communication problem will occur.
One interface can be configured with two or more IP addresses. To configure multiple IP addresses, you can use the **secondary** parameter.

Configuration Examples The following example sets the IP address on the Ethernet interface.

```
Ruijie(config)#interface fastethernet 0/0
Ruijie(config-line)#ip address 192.168.12.1 255.255.255.0
```

Related Commands

Command	Description
ip unnumbered	Borrows the IP address of other interfaces.

Platform Description N/A

ip unnumbered

Use this command to borrow the IP address of another interface in interface configuration mode. Use the **no** form of this command to remove this setting.
ip unnumbered *type interface-number*
no ip unnumbered

Parameter Description

Parameter	Description
type	Interface type
interface-number	Corresponding interface number of an interface type

Defaults N/A

Command Mode Interface configuration mode

Usage Guide You can borrow IP addresses from different interfaces. In some solutions, for example, the dial-up backup solution, sometimes only one IP address is needed in the primary interface and backup interface. In this case, the primary interface and backup interface can borrow the IP address of the Loopback interface. The following table shows the interface type whose IP address can be borrowed.

Type	Interface Type
Dialer	Logical dialer interface
Fastethernet	10/100M fast Ethernet interface
loopback	Loopback interface
Null	Null interface

Configuration Examples The following example borrows the IP address (*192.168.12.1/24*) of the Loopback 0 interface for serial interface 1/0.

```
Ruijie(config)# loopback 0
Ruijie(config-if)# ip address 192.168.12.1 255.255.255.0
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# ip unnumbered loopback 0
```

Related Commands

Command	Description
keep-period	Interval at which the RGOS sends keepalive packets (in seconds). The value 0 indicates that the RGOS will not send keepalive packets. The default value is 10s, and the configurable range is from 1 to 32767.

Platform Description N/A

keepalive

Use this command to transmit keepalive packets. Use the **no** form of this command to disable the keepalive function.

keepalive [*keep-period* [*keep-retries*]]

no keepalive

Parameter Description

Parameter	Description
keep-period	Interval at which the RGOS sends keepalive packets (in seconds). The value 0 indicates that the RGOS will not send keepalive packets. The default value is 10s, and the configurable range is from 1 to 32767.
keep-retries	This option means the maximum number of timeout, in the range from 1 to 255, the default value is shown as below: Tunnel interface: 3 HDLC protocol: 3 PPP protocol: 10

Defaults By default, the Ethernet interface is not enabled with the keepalive function.

For other WAN interfaces, different WAN link layer protocols have different keepalive periods.

Command Mode Interface configuration mode

Usage Guide On WAN network interfaces, the encapsulated link layer protocol basically enables this function for normal operations. By configuring this command, you can set the keepalive period of the link layer protocol to control the time for sending keepalive packets.
On the tunnel interface and the interfaces encapsulated the HDLC or PPP protocol, the maximum timeout number of the keepalive packet can be set. If no response is received by the keepalive packet in the maximum timeout number, the connection created will be disconnected.

Configuration Examples The following example sets the maximum timeout number of the keepalive packet to 3.

```
Ruijie# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface serial 3/0
Ruijie(config-if)# keepalive 10 3
Ruijie(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

linecode

Use this command to set the line codec format of the CE1 interface. Use the **no** form of this command to restore the default setting.
linecode hdb3
no linecode

Parameter Description

Parameter	Description
hdb3	Sets the line codec format to HDB3.

Defaults The default value is HDB3.

Command Mode CE1 interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the line codec format of the CE1 interface to HDB3.

```
Ruijie(config-controller)# linecode hdb3
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

loopback

Use this command to enable local loopback or remote loopback on a CE1 interface. Use the **no** form of this command to remove this setting.

loopback { **local** | **remote** }

no loopback { **local** | **network** }

Parameter Description

Parameter	Description
local	Local loopback
remote	Remote loopback
network	Remote loopback.

Defaults Local loopback is disabled by default.

Command Mode CE1 Interface configuration mode

Usage Guide This command is configured for tests of some special functions..

Configuration Examples The following example enables local loopback on a CE1 interface.

```
(config-controller)# loopback local
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **loopback** { **local** | **network** } command is supported on RSR30-X series router.

loopback local

Use this command to set the loopback mode of the E1 interface. Currently, only the local loopback mode is supported. Use the **no** form of this command to remove this setting and restore the normal working mode.

loopback local

no loopback

Parameter Description

Parameter	Description
N/A	N/A

Defaults Local loopback is disabled by default.

Command Mode E1 interface configuration mode

Usage Guide You need to configure the E1 interface to work in local loopback mode only when you test some special functions. This command is valid only when the controller port is set to the E1 mode.

Configuration Examples The following example sets the E1 interface to work in local loopback mode.
Ruijie(config-controller)# **loopback local**

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mac-address

Use this command to set the physical MAC address on an interface. Use the **no** form of this command to remove this setting.
mac-address *H.H.H*
no mac-adderss

Parameter Description

Parameter	Description
H.H.H	MAC address, in hex format; each H is of two bytes, so this parameter is of 6 bytes, namely 48 bits.

Defaults The factory setting is used by default.

Command Mode Interface configuration mode

Usage Guide Each Ethernet interface has a globally unique MAC address. If necessary, you can modify the MAC address of the Ethernet interface, but you must ensure that it is unique in the LAN. The setting of the MAC address may affect the communication within the LAN. If not necessary, you are recommended not to configure the MAC address.

Configuration Examples The following example sets the MAC address on the Ethernet interface.

```
Ruijie(config)# interface fastethernet 0/0
Ruijie(config-if)# mac-address 00d0.f8fb.110d
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

media-type

Use this command to set the physical media type on the Gigabit Ethernet interface. Use the **no** form of this command to restore the default setting.

media-type { **baset** | **basex** }

no media-type

Parameter Description

Parameter	Description
baset	Allows the Gigabit Ethernet interface to use twisted pair cables only.
basex	Allows the Gigabit Ethernet interface to use optical fibers only.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mtu

Use this command to set the MTU (Maximum Transmission Unit) of the Ethernet interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

mtu *size*

no mtu

Parameter Description

Parameter	Description
size	Size of the MTU, which is equal to or larger than 64 bytes. The upper limit of the MTU size depends on the interface type. The default value is 1500 bytes.

Defaults The size of the MTU is 1500 bytes.

Command Mode Interface configuration mode

Usage Guide The setting of the MTU may affect the throughput and delay of the network, so it should be set appropriately according to the service application and bandwidth. Sometimes multiple services are used in a mixed way, and one of the services must be highly real time and the data length is small, like voice transmission; while the data of another service does not need to be real time, and the data length is large, which will occupy enormous bandwidth resources, like FTP data transmission. In this case, you can set the MTU to a small value for even allocation of the bandwidth over different service data.

Configuration Examples The following example sets the MTU to 576 for sync interface 1/0.

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# mtu 576
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command may cause a problem to RSR30 series products. The RAID Gigabit Ethernet interface of the RSR30 series products will not regard the data less than 1518 bytes as the overlength frame. If the MTU is set less than 1518 bytes, the Ethernet frame with the length being longer than the configured MTU and less than 1518 bytes will not be counted as the overlength frame (the Ethernet frame is counted as the giant type on the interface of CLI command line.)

shutdown

Use this command to shut down the specified interface in interface configuration mode. Use the **no**

form of this command to restart an interface.

shutdown

no shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command can be used to invalidate an interface. When you use this command on a sync serial interface, the DTR and RTS are directly disabled. If the external modem has DTR or RTS signal indicators, they will go off, and the sync interface indicator on the device also goes off.

If an interface is shut down, you can use the **show interface** command to view the "is administratively down" prompt.

Configuration Examples The following example shuts down sync serial port 1/1.

```
Ruijie(config)# interface serial 1/1
Ruijie(config-if)# shutdown
%LINK CHANGED: Interface serial 1/1, changed state to administratively down
```

Related Commands

Command	Description
show interface	Shows the hardware statistics and link communication status of an interface.

Platform Description N/A

speed

Use this command to set the speed of the Ethernet interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

speed {10 | 100 |1000| auto }

no speed

Parameter Description

Parameter	Description
10	Sets the speed of the Ethernet interface to 10M.
100	Sets the speed of the Ethernet interface to 100M.
1000	Sets the speed of the Ethernet interface to 1000M.

auto	Sets auto mode for the Enternet interface that the system automatically configures the interface to work in the 10M, 100M or 1000M mode according to the actual conditions of the hub, Layer 2 device, and network interface adapter connected with the interface. The optical interfaces of the S2028G/S2052G/S25/M86-24SFP can work at 100M. The gigabit SFP interfaces of other devices can work only at 1000M.

Defaults The auto mode is used by default.

Command Mode Interface configuration mode

Usage Guide To enable the adaptive function of the network interface, you should execute the **speed** and **duplex** commands, that is, the duplex mode and 10/100M rate adaptation. The functions of the **duplex** and **speed** commands are shown in the following table:

duplex	speed	Working Mode
full	10	Work in 10M full duplex mode.
Full	100	Work in 100M full duplex mode.
Half	10	Work in 10M half duplex mode.
Half	100	Work in 100M half duplex mode.
Auto	Auto	Work in adaptive mode.

Configuration Examples The following example sets Fast Ethernet interface 0/0 to work in 10/100M adaptive mode.

```
Ruijie(config)#interface fastethernet 0/0
Ruijie(config-if)#speed auto
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

using

Use this command to set the working mode of the CE1 interface. Use the **no** form of this command to restore the default setting.

using { **e1 | ce1** }

no using

Parameter Description

Parameter	Description
e1	E1 working mode
ce1	CE1 working mode

Defaults The CE1 working mode is used by default.

Command Mode CE1 interface configuration mode

Usage Guide When the CE1 interface is set to the E1 working mode, it is equivalent to an interface without timeslots divided and with a bandwidth of 2048000 bps. Its logical feature is the same as the sync serial port.
When the CE1 interface is set to the CE1 working mode, it can be divided into 32 timeslots numbering 0 to 31. Timeslot 0 is used to transmit the frame synchronization signal, and timeslots 1-31 can be allocated to several specified channel-groups. The channel groups allocated with timeslots are equivalent to several interfaces, and their logical features are the same as the synchronization serial port.

Configuration Examples The following example sets the CE1 interface to work in E1 mode.

```
Ruijie(config-controller)# using e1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

tunnel checksum

Use this command to implement the integrity check of the interface data in interface configuration mode. Use the **no** form of this command to remove this setting.
tunnel checksum
no tunnel checksum

Parameter Description

Parameter	Description
N/A	N/A

Defaults Data integrity check is disabled by default.

Command Interface configuration mode

Mode

Usage Guide This command is only applicable to the interfaces of GRE (Generic Route Encapsulation). Some encapsulated protocols add the checksum at the end of the data packet. In this case, the tunnel interface must perform the checksum check, and the damaged packet will be directly discarded.

Configuration Examples The following example configures the **checksum** command on the tunnel 0 interface.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel checksum
```

Related Commands

Command	Description
show interface tunnel	Shows the related information of the tunnel interface.

Platform Description N/A

tunnel destination

Use this command to set the destination IP address for the specific interface in interface configuration mode. Use the **no** form of this command to remove this setting.

tunnel destination *ip*-address

no tunnel destination

Parameter Description

Parameter	Description
ip-address	Destination IP address of the tunnel

Defaults The destination IP address is null.

Command Mode Interface configuration mode

Usage Guide This command allows you to specify the remote IP address of the tunnel to be established. Without this necessary setting, the tunnel cannot be established.

Configuration Examples The following example sets the destination IP address to 61.154.101.3 on the tunnel 0 interface.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel destination 61.154.101.3
```

Related Commands

Command	Description
show interface tunnel	Shows the related information of the tunnel

	interface.

Platform Description N/A

tunnel key

Use this command to set the security key of the tunnel interface, which must be an integer. Use the **no** form of this command to remove the key.

tunnel key *value*

no tunnel key

Parameter Description

Parameter	Description
value	Value of the tunnel key, in the range from 0 to 4294967295

Defaults No key is configured by default.

Command Mode Interface configuration mode

Usage Guide If a tunnel is established without a key for protection, it may be vulnerable to illegal intrusion and attacks. The **tunnel key** command only takes effect on the GRE encapsulation.

Configuration Examples The following example sets the 1234 key on the tunnel 0 interface.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel key 1234
```

Related Commands

Command	Description
show interface tunnel	Shows the related information of the tunnel interface.

Platform Description N/A

tunnel mode

Use this command to set the encapsulation mode on the tunnel interface. Use the **no** form of this command to restore the default setting.

tunnel mode { **gre { ip | ipv6 }**| **ipip** | **ipv6ip** [**6to4 | isatap**] }

Parameter

Parameter	Description

Description

gre ip	GRE (Generic Route Encapsulation) on the IP layer
gre ipv6	GRE (Generic Route Encapsulation) on the IPv6 layer
ipip	IP over IP encapsulation mode
ipv6ip	IPv6 over IP encapsulation mode

Defaults The gre ip mode is used on the router.

Command Mode Interface configuration mode

Usage Guide The encapsulation mode for a tunnel interface is the carrier protocol of the tunnel. By default, the tunnel interface uses the GRE encapsulation mode. Certainly, you can also determine the encapsulation mode of the tunnel interface according to the actual condition. By default, you can implement the GRE of the IP tunnel without defining the encapsulation mode.

Configuration Examples The following example encapsulates IP with GRE on the tunnel 0 interface.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
show interface tunnel	Shows the related information of the tunnel interface.

Platform Description N/A

tunnel source

Use this command to set the source IP address of the tunnel interface in interface configuration mode. Use the **no** form of this command to remove this setting

tunnel source { *ip-address* | *interface-type interface-number* }

no tunnel source

Parameter Description

Parameter	Description
ip-address	Source IP address of the tunnel interface, this is, the IP address of another interface set on the device
interface-type	General interface type, for example, Async, Dialer, Ethernet, FastEthernet, Loopback, Null and other Tunnel interfaces
interface-number	Interface number

Defaults No source IP address is configured by default.

Command Mode Interface configuration mode

Usage Guide When the tunnel interface is used, you must specify the source IP address.

Configuration Examples The following example specifies serial interface 1/0 as the source IP address of the tunnel 0 interface.

```
Ruijie(config)#interface tunnel 0
Ruijie(config-if)#tunnel source serial 1/0
```

Related Commands

Command	Description
show interface tunnel	Shows the related information of the tunnel interface.

Platform Description N/A

show controller e1

Use this command to view the related information of the CE1 interface.

show controller e1 [*slot/port*]

Parameter Description

Parameter	Description
slot	Number of the slot where the E1 controller resides
port	Number of the port of the slot where the E1 controller resides

Defaults N/A

Command Mode Privileged user mode

Usage Guide This command shows the related information of all CE1 interfaces or the specified CE1 interface, including the physical status, working mode, frame check mode, line codec format, and sync clock source information.

If no CE1 interface is specified, the command output shows the total statistics of the current 15 minutes and in the past 24 hours.

If a CE1 interface is specified, the command output shows the total statistics of the current 15 minutes, each 15 minutes in the past 24 hours, and of the past 24 hours.

Configuration The following example shows the related information of all the CE1 interfaces.

Examples

```
Ruijie#show controller e1
E1 1/1/0 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
E1 1/1/1 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
E1 1/1/2 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
E1 1/1/3 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
```

```
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
E1 1/1/4 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
E1 1/1/5 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
E1 1/1/6 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
E1 1/1/7 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
```

```
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (446 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following example shows the related information of the specified CE1 interface.

```
Ruijie# show controller e1 1/1/0
E1 1/1/0 is down.
Applique type is Channelized E1 - balanced
Receiver has no alarms.
Framing is crc4, Line Code is hdb3, Clock Source is line
Data in current interval (458 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 1:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 2:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 3:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 4:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 5:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 6:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 7:
```

```
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 8:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 9:
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 9 fifteen minute intervals):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show interface

Use this command to view the status and statistics of the specified interface in privileged or common user mode.

show interface *type interface-number*

Parameter Description

Parameter	Description
type	Interface type
interface-number	Interface number

Defaults N/A

Command Mode Privileged user mode or common user mode

Usage Guide You can use the **show interface** command to view the following information: interface and protocol status, MTU, bandwidth, loopback status, interface queue policy and usage, protocol communication, interface packet input/output and error, and link physical status. You can see that this command is the most commonly used one in checking the usage of the data link layer on an interface.

On a low-speed interface, the default queue policy is WFQ.

On a high-speed interface, when the default policy is the FIFO queue policy, you can use the **show interface** command to see the usage of the queue: Queueing strategy: fifo Output queue 0/40, 0 drops; input queue 0/75, 0 drops; currently the output queue uses 0, with the maximum of 40, packet drop of 0; the input queue currently uses 0, with the maximum of 75, packet drop of 0.

Configuration Examples

The following example shows the information of the FastEtheret 0/0 interface.

```
Ruijie#show interface fastEthernet 0/0
FastEthernet 0/0 is UP  , line protocol is UP
Hardware is Nat-Semi DP83815DVNG FastEthernet, address is 0a0b.0c0d.0e0f (bia
0a0b.0c0d.0e0f)
Interface address is: no ip address
ARP type: ARPA,ARP Timeout: 3600 seconds
MTU 1500 bytes, BW 100000 Kbit
Encapsulation protocol is Ethernet-II, 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 0/40, 0 drops;
Input queue 0/75, 0 drops
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
782 packets input, 88920 bytes, 0 no buffer
Received 782 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
```

The following example shows the information of the sync serial interface.

```
Ruijie# show interface serial 1/0
serial 1/0 is UP  , line protocol is UP
Hardware is Infineon DSCC4 PEB20534 H-10 serial
Interface address is: 1.1.1.2/24
MTU 1500 bytes, BW 2000 Kbit
Encapsulation protocol is FRAME RELAY, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
RXload is 1 ,Txload is 1
LMI enq sent  1087, LMI status recvd 1026, LMI update recvd 0, DTE LMI up
LMI enq recvd 8, LMI status sent  0, LMI update sent  0
LMI DLCI 0  LMI type is CCITT, frame relay DTE  interface broadcasts 0
Queueing strategy: WFQ
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
1194 packets input, 20226 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
2052 packets output, 37755 bytes, 0 underruns
0 output errors, 0 collisions, 809 interface resets
11 carrier transitions
V35 DCE cable
DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show vlans

Use this command to view the information of the VLAN interface in privileged EXEC mode.

show vlans [*VLANID* **]**

Parameter Description

Parameter	Description
VLANID	ID of the VLAN

Defaults If no VLAN ID is specified, the command output shows the statistics of all VLAN interfaces.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows a typical output of executing this command.

```
Ruijie# show vlans
Virtual LAN ID:  3 (IEEE 802.1Q Encapsulation)
vLAN Interface FastEthernet 0/0.1
IP address: 1.1.1.1
Received:30 packets,
Transmitted: 30 packets
Virtual LAN ID:  4 (IEEE 802.1Q Encapsulation)
VLAN Interface FastEthernet 0/0.2
IP address: 1.1.2.1
Received:0 packets,
Transmitted: 0 packets
```

The following presents the description of parameters:.

```
Virtual LAN ID: ID of the VLAN
VLAN interface: Interface running the VLAN
Address: IP address of the interface
Received: Number of received packets
Transmitted: Number of transmitted packets
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

VLAN Commands

add

Use this command to add one or a group Access interface into current VLAN. Use the **no** form of the command to remove the Access interface.

add interface { *interface-id* | **range** *interface-range* }

no 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.

Default configuration

All layer-2 Ethernet interfaces are in the VLAN1.

Command mode

VLAN configuration mode.

Usage guidelines

- 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** v*lan-id*). 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.

Examples

The following example adds the interface GigabitEthernet 0/10 into the 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 into the 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 into the 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**	Show the layer-2 interfaces.

name

Use the command to specify the name of a VLAN. Use the **no** form of the command to restore it to the default setting.

name *vlan-name*

no name

Parameter description

Parameter	Description
vlan-name	VLAN name

Default configuration	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 guidelines	You can view the VLAN settings by using the **show vlan** command.
Examples	`Ruijie(config)# vlan 10` `Ruijie(config-vlan)# name vlan10`

Related commands

Command	Description
show vlan	Show member ports of the VLAN.

switchport access

Use this command to configure an interface as a statics 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.

Default configuration	By default, the switch port is an access port and the VLAN is VLAN 1.
Command mode	Interface configuration mode.
Usage guidelines	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.
Examples	`Ruijie(config)# interface gigabitethernet 1/1` `Ruijie(config-if)# switchport access vlan 2`

Related commands

Command	Description
switchport mode	Specify the interface as Layer 2 mode (switch port mode).
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

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 the command to restore the default setting.

switchport mode {**access** | **trunk | hybrid | uplink | dot1q-tunnel**}

no switchport mode

Parameter description

Parameter	Description
access	Configure the switch port as an access port.
trunk	Configure the switch port as a trunk port.
hybrid	Configure the switch port as a hybrid port.
uplink	Configure the switch port as an uplink port.
dot1q-tunnel	Configure the switch port as a 802.1Q tunnel port.

Default configuration

By default, the switch port is an access port.

Command mode

Interface configuration mode.

Usage guidelines

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.

Examples

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

Related commands	Command	Description
	switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.
	switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of the 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*	Configure 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*	Specify the native VLAN.

Default configuration	The default allowed-VLAN list is all the VLANs, the default native VLAN is VLAN 1.
Command mode	Interface configuration mode.

Usage guidelines

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 port by configuring allowed VLAN lists on a trunk port .

Use **show interfaces switchport** to display configuration.

Examples

The example below 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
Interface Switchport Mode Access Native Protected VLAN lists
--------- --------- --------- ---------
FigabitEthernet 1/15  enabled  TRUNK  1   1   Disabled  1,3-4094
```

Related commands

Command	Description
show interfaces	Show the interface information.
switchport access	Use this command to configure an interface as a statics access port and assign it to a VLAN.

vlan

Use this command to enter the VLAN configuration mode. Use the **no** form of the command to remove the VLAN.

vlan vlan-id

no vlan *vlan-id*

Parameter description

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

Command mode

Global configuration mode.

Usage guidelines

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

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

Examples

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

Related commands

Command	Description
show vlan	Show member ports of the VLAN.

show vlan

Show member ports of the VLAN.

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

Parameter description

Parameter	Description
vlan-id	VLAN ID

Default configuration

Show all the information by default.

Command mode

Privileged EXEC mode.

Usage guidelines

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

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

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	Add the interface to a VLAN.

Aggregate Port Commands

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** }

no aggregateport load-balance

Parameter Description

Parameter	Description
dst-mac	Load balance based on the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
src-mac	Load balance based on the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-ip	Load balance based on the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
dst-ip	Load balance based on the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Load balance based on the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-mac	Load balance based on the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.

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

.

Command Mode Global 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 N/A

aggregateport member linktrap

Use this command to configure LinkTrap for 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 N/A

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

port-group

Use this command to assign a physical interface to be a member port. Use the **no** form of this

command to restore the default setting.

port-group *port-group-number*

no port-group

Parameter Description

Parameter	Description
port-group-number	Member group ID of an aggregate port, the interface number of the aggregate port.

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 AP member 3.

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# port-group 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description RSR20-X-28 router supports up to 6 aggregate ports and 8 AP member ports.

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 Privileged EXEC mode

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

Configuration The following example displays the aggregate port configuration.

Examples

```
Ruijie# show aggregateport 1 summary
AggregatePort    MaxPorts            SwitchPort Mode       Load balance                  Ports
-------------    ---------- ---------- ------    ----------------------------- ------------------------
Ag1                 8                  Enabled       ACCESS    dst-mac                       Gi0/2
```

Related Commands

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

Platform Description N/A

RMON Commands

rmon alarm

Use this command to monitor a MIB variable. The **no** form of this command cancels the logging.

rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]

no rmon alarm *number*

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-threadhold/falling-threadhold**, 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*]	Add an event definition.

rmon event

Use this command to define an event. The **no** form of this command cancels the logging.

rmon event *number* [**log**] [**trap** *community*] [*description-string*] [**description** *description-string*] [**owner** *owner-name*]

no rmon alarm *number*

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(config)# rmon event 1 log trap rmon description "ifInNUcastPkts is too much " owner zhangsan`

Related commands

Command	Description
rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry.

show rmon alarm

Use this command to show the rmon alarm table.

show rmon alarm

Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.

Examples	The example below shows the rmon alarm table.
	`Ruijie# show rmon alarm`
	`rmon alarm table:`
	`index: 10,`
	`interval: 30,`
	`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: zhangesan,
stats: 1,
```

Related commands

Command	Description
rmon alarm number variable interval {**absolute** | **delta** } **rising-threshold** value [event-number] **falling-threshold** value [event-number] [**owner** ownername]	Add an alarm entry.

show rmon event

Use this command to show the event information.

show rmon event

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples

The example below shows the event information.

```
Ruijie#  show rmon event
rmon event table:
                index = 1
                description = ifInNUcastPkts
                type = 4
                community = rmon
                lastTimeSent = 0 d:0 h:0 m:0 s
                owner = zhangsan
                status = 1
```

	Command	Description
Related commands	**rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	Add an event entry.

SPAN Commands

monitor session

Use this command to configure the SPAN session and specify the source port (monitored port).
monitor session *session-num* **source interface** *interface-id* [**both** | **rx** | **tx**]

Use this command to configure the SPAN session mirroring only the traffic permitted by the access list
monitor session *session-num* **source interface** *interface-id* **rx acl** *acl-name*

Use this command to configure the SPAN session and specify the destination port (monitoring port).
monitor session *session-num* **destination interface** *interface-id* [**encapsulation** | **switch**]

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 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
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	Enables switching on the destination port. Switching function is disabled by default.

Defaults Port monitoring is disabled by default.

Command mode Global configuration mode.

Usage Guide Use this command to configure SPAN or remote SPAN, and specify the source port or destination port.
If the **both**, **rx** or **tx** is not specified for the source port, the **both** parameter is the default.
Configuring an access list for the source port indicates that only the traffic permitted by the access list is monitored.
The **switch** and **encapsulation** 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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

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

IP Address and Service Commands

IP Address Configuration Commands

ip-address

Use this command to configure the IP address of an interface. Use the **no** form of this command to delete the IP address of the interface.

ip address *ip-address network-mask* [**secondary**] | [**gateway** *ip-address*]

no ip address [*ip-address network-mask* [**secondary**] | [**gateway**]]

Parameter Description

Parameter	Description
ip-address	32-bit IP address, which comprises multiple groups of 8 bits in decimal format. Groups are separated by dots.
network-mask	32-bit network mask, which comprises multiple groups of 8 bits in decimal format. 1 stands for the mask bit, and 0 stands for the host bit. Groups are separated by dots.
secondary	Indicates the secondary IP address that has been configured.
gateway *ip-address*	Configures the gateway address for the Layer-2 switch. The gateway address is only supported on Layer-2 switches. No address follows the gateway parameter when using the no form of this command.

Defaults No IP address is configured for the interface.

Command Mode Interface configuration mode

Usage Guide The device 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 of the IP address is the network address portion. Among the network mask, the IP address bits set to 1s are the network address portion. The IP address bits that set to 0s are the host address. For example, the network mask of a 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 as the network address portion, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called a subnet mask.

The RGOS software supports multiple IP addresses for an interface. One is the primary IP address and the others are secondary IP addresses. Theoretically, there is no limit on the number of secondary IP addresses. The primary IP address, however, must be configured before the secondary IP addresses are configured. The secondary IP addresses and the primary IP address must belong to different networks, and different secondary IP addresses must also belong to 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 does not have enough host addresses. At present, a 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 L2-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 is configured with 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 using the **ip default-gateway** command. Sometimes the Layer-2 switch may be managed through Telnet, and the management IP address and default gateway of the Layer-2 switch need to be modified. In this case, after configuring either of the **ip address** and **ip default-gateway** commands, the other command cannot be configured any more due to the configuration change which causes a failure to access this device through the network. So you need to use the keyword ***gateway*** in the **ip address** command to modify both the management IP address and the default gateway. The keyword ***gateway*** is not in the output of the **show running config** command but in the output of the **ip default-gate** command.

Configuration Examples

The following example sets the primary IP address to 10.10.10.1, and the network mask to 255.255.255.0.

```
ip address 10.10.10.1 255.255.255.0
```

The following example sets the default gateway to 10.10.10.254.

```
ip address 10.10.10.1 255.255.255.0 gateway 10.10.10.254
```

Related Commands

Command	Description
show interface	Shows detailed information about the interface.

Platform Description

For the Layer 2 switch, the IP address can be configured only for a Layer 3 interface. The Level-2 address is not supported, that is, the secondary IP address option is unavailable.

The keyword ***gateway*** is only supported by Layer-2 switches.

ip unnumbered

Use this command to configure an unnumbered interface. After an interface is configured as an unnumbered interface, it is allowed to run the IP protocol and can receive and send IP packets. Use the **no** form of this command to cancel this configuration.

ip unnumbered *interface-type interface-number*

no ip unnumbered

Parameter

Parameter	Description

Description

interface-type	Interface type
interface-number	Interface number

Defaults No unnumbered interface is configured.

Command Mode Interface configuration mode

Usage Guide An unnumbered interface is an interface on which IP is enabled but no IP address is assigned to it. The unnumbered interface should be associated to an interface with an IP address. The source IP address of the IP packet generated by 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 an unnumbered interface according to the IP address of the associated interface. The following restrictions apply when an unnumbered interface is used:
(1) An Ethernet interface cannot be configured as an unnumbered interface.
(2) A serial interface can be configured as an unnumbered interface when it is encapsulated with SLIP, HDLC, PPP, LAPB and Frame Relay. However, when Frame Relay is used for encapsulation, only the point-to-point interface can be configured as an unnumbered interface. X.25 encapsulation does not allow configuration as an unnumbered interface.
(3) You cannot detect whether an unnumbered interface works normally using the **ping** command, because no IP address is configured for the unnumbered interface. However, the status of the unnumbered interface can be monitored remotely using SNMP.
(4) The network cannot be started using an unnumbered interface.

Configuration Examples The following example configures the local interface as an unnumbered interface, and sets the associated interface to the FE interface 0/1. An IP address must be configured for the associated interface.

```
ip unnumbered fastEthernet 0/1
```

Related Commands

Command	Description
show interface	Shows detailed information about the interface.

Platform Description This command is not supported on Layer 2 switches.

peer default ip address

Use this command to assign an IP adddress to the peer end for PPP negotiation. Use the **no** form of this command to cancel this configuration.
peer default ip address { *ip-address* | **pool** [*pool-name*] }
no peer default ip address

Parameter Description

Parameter	Description
ip-address	The IP address to be assigned to the peer end
pool-name	(Optional) Specifies the name of the address pool from which the IP address is assigned. If this parameter is not specified, the IP address will be assigned from the default address pool.

Defaults No IP address is assigned to the peer end on the interface.

Command Mode Interface configuration mode

Usage Guide When the peer interface is not configured with an IP address but the local device has been configured with an IP address, the local device can be configured to assign an IP address for the peer interface. In this case, the **ip address negotiation** command should be configured on the peer device and the **peer default ip address** command should be configured on the local device, so that the peer interface accepts the IP address assigned through PPP negotiation.
This command can be configured only in a point-to-point interface encapsulatedwith the PPP or SLIP protocol.
The **peer default ip address pool** command is used to assign an IP address to the peer end from an IP address pool which is configured through the **ip local pool** command.
The **peer default ip address** *ip-address* command is used to directly specify an IP address for the peer end. This command cannot be configured on a virtual template interface or asynchronous interface.

Configuration Examples The following example sets the IP address assigned to the peer end on the interface Serial 4/1/10:13 to 10.0.0.1.

```
interface Serial 4/1/10:13
peer default ip address 10.0.0.1
```

Related Commands

Command	Description
ip local pool	Configures the IP address pool.

Platform Description This command is not supported on switches.

arp

Use this command to add a permanent IP-MAC address mapping to the ARP cache table. Use the **no** form of this command to delete the static MAC address mapping.
arp [**vrf** *name*] *ip-address MAC-address type*
no arp [**vrf** *name*] *ip-address*

Parameter Description

Parameter	Description
vrf *name*	Specifies the VRF instance. The *name* parameter indicates the name of the VRF instance.
ip-address	The IP address that corresponds to the MAC address. It comprises four groups 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 Ethernet interfaces.

Defaults There is no static mapping record in the ARP cache table.

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 an Ethernet host.

```
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

arp anti-ip-attack

For a message that hits a directly-connected route, if the switch does not learn the ARP entry that corresponds to the destination IP address, the switch is not able to forward the message via hardware and needs to send the message to the CPU to parse the address. This process is called ARP learnning. Sending a large number of such messages to the CPU, however, will influence the other tasks of the switch. To prevent the IP messages from attacking the CPU, a discard entry is set to the hardware during address resolution, so that all sequential messages with that destination IP address are not sent to the CPU at all. After the address resolution, the entry is updated to the forwarding status, so that the switch can forward the messages with that destination IP address via hardware.

In general, during the ARP request ,if the switch CPU receives three destination IP address messages that hit the ARP entry, the switch considers that there is possibility to attack the CPU and thus sets a discard entry to prevent unknown unicast messages from attacking the CPU. Users can set the *num* parameter of this command to decide whether it attacks the CPU in the specific network

environment or disable this function. Use the **arp anti-ip-attack *num*** command to set the parameter or disable this function. Use the **no** form of this command to restore the *num* parameter to the default value 3.

arp anti-ip-attack *num*

no arp anti-ip-attack

Parameter Description

Parameter	Description
num	The number of IP messages to trigger the ARP to set a discard entry. The value ranges from 0 to 100. 0 stands for disabling the ARP anti-IP-attack function.

Defaults The switch sets a discarded entry after three unknown unicast messages are sent to the CPU.

Command Mode Global configuration mode

Usage Guide The ARP anti-IP-attack function will occupy the switch hardware routing resources when the switch is attacked by unknown unicast messages. If there are enough resources, you can set the *num* parameter in the **arp anti-ip-attack** to a smaller value. If not, in order to first ensure normal routing, you can set the *num* parameter to a larger value or simply disable this function.

Configuration Examples The following example sets the number of IP messages that will trigger ARP to set a discard entry to 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 This command is supported on Layer 3 switches.

arp gratuitous-send interval

Use this command to set the interval of sending free ARP request messages on an interface. Use the **no** form of this command to disable this function on the interface.

arp gratuitous-send interval *seconds*

no arp gratuitous-send

Parameter Description

Parameter	Description

seconds	The time interval in seconds for sending free ARP request messages in the range from 1 to 3600

Defaults Periodically sending free ARP request messages is disabled on an interface.

Command Mode Interface configuration mode

Usage Guide If a network interface of the switch is used as the gateway of its downlink devices but a downlink device pretends to be the gateway, you can configure the function to send free ARP request messages regularly on this interface to notify that the switch is the real gateway.

Configuration Examples The following example sets the interval for sending free ARP request messages to SVI 1 to 1 second.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# arp gratuitous-send interval 1
The following example disables the function of sending free ARP request messages 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

arp retry interval

Use this command to set the interval for sending ARP request messages locally, namely, the time interval between two continuous ARP requests sent for parsing one IP address. Use the **no** form of this command to restore the default value, that is, retry an ARP request per second.

arp retry interval *seconds*

no arp retry interval

Parameter Description

Parameter	Description
seconds	Time interval in seconds for retrying ARP request messages in the range from 1 to 3600 1 second by default

Defaults The retry interval of ARP requests is 1 second.

Command Global configuration mode

Mode

Usage Guide The switch sends ARP request messages frequently, thus causing problems like network congestion. In this case, you can set the retry interval of ARP request messages to a larger value. In general, it should not exceed the aging time of dynamic ARP entries.

Configuration Examples The following example sets the retry interval of ARP request messages to 30 seconds.
arp retry interval 30

Related Commands

Command	Description
arp retry times *number*	Sets the retry times of ARP request messages.

Platform Description N/A

arp retry times

Use this command to set the local retry times of ARP request messages, namely, the times of sending ARP request messages to parse one IP address. Use the **no** form of this command to restore the default settings (five ARP requests).
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 to 100. 1 indicates that the ARP request is not retransmitted but only one ARP request message is sent.

Defaults If the ARP response message is not received, the ARP request message will be sent for 5 times, and then timeout occurs.

Command Mode Global configuration mode

Usage Guide The switch sends ARP request messages frequently, thus causing problems like network congestion. In this case, you can set the retry times of ARP request messages to a smaller value. In general, the retry times should not be set to an excessively large value.

Configuration Examples The following example sets the retry times of local ARP request messages to 1.

```
arp retry times 1
```

The following example sets the retry times of local ARP request messages to 2.

```
arp retry times 2
```

Related Commands

Command	Description
arp retry interval *seconds*	Sets the retry interval of ARP request messages.

Platform Description N/A

arp timeout

Use this command to configure the timeout for ARP static mapping records in the ARP cache. Use the **no** form of this command to restore the default settings.

arp timeout *seconds*

no arp timeout

Parameter Description

Parameter	Description
seconds	The timeout in seconds ranging from 0 to 2147483

Defaults The default timeout is 3600 seconds.

Command Mode Interface configuration mode

Usage Guide The ARP timeout setting is only applicable to the IP and MAC address mapping records 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 ARP. Therefore, weight the advantages and disadvantages of ARP timeout before using it. Generally you do not need to configure the ARP timeout unless specially required.

Configuration Examples The following example sets the timeout for dynamic ARP mapping records that are learned dynamically from FE port 0/1 to 120 seconds.

```
interface fastEthernet 0/1
arp timeout 120
```

Related Commands

Command	Description
clear arp-cache	ClearS the ARP cache table.
show interface	Shows interface information.

Platform Description N/A

arp unresolve

Use this command to configure the maximum number of unresolved ARP entries. Use the **no** form of this command to restore the default value 8192.

arp unresolve *number*

no arp unresolve

Parameter Description

Parameter	Description
number	The maximum number of unresolved ARP entries in the range from 1 to 8192. The default value is 8192.

Defaults The ARP cache table can contain up to 8192 unresolved entries.

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, use this command to limit the number of unresolved entries.

Configuration Examples The following example sets the maximum number of unresolved entries to 500.

```
arp unresolve 500
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip proxy-arp

Use this command to enable the proxy ARP funtion on the interface. Use the no form of this command to disable the proxy ARP function.

ip proxy-arp

no ip proxy-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The proxy ARP function is disabled on L3 switches of 10.2(3) and later versions, but enabled on routers.

Command Mode Interface configuration mode

Usage Guide Proxy ARP helps hosts without routing information to obtain MAC addresses of other networks or subnet IP addresses. For example, a device receives an ARP request. The IP addresses of the request sender and receiver are in different networks. However, the device knows a route to the IP address of the request receiver and sends an ARP response, in which the MAC address is the Ethernet MAC address of the device itself. This process is known as proxy ARP.

Configuration Examples The following example enables proxy ARP on FE port 0/1.

```
interface fastEthernet 0/1
ip proxy-arp
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

ip broadcast-addresss

Use this command to define a broadcast address for an interface in interface configuration mode. Use the **no** form of this command to cancel the broadcast address configuration.

ip broadcast-addresss *ip-address*

no ip broadcast-addresss

Parameter Description

Parameter	Description
ip-address	Broadcast address of the IP network

Defaults The IP broadcast address is 255.255.255.255.

Command Mode Interface configuration mode

Usage Guide At present, the destination address of an IP broadcast packet is all-1s, indicating 255.255.255.255. The RGOS software can generate broadcast packets with other defined IP addresses, and can receive both all-1s packets and broadcast packets defined by itself.

Configuration Examples The following example sets the destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```
ip broadcast-address  0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in interface configuration mode. Use the **no** form of this command to cancel the configuration.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter Description

Parameter	Description
access-list-number	(Optional) Access list number ranging from 1 to 199 or from 1300 to 2699. After an access list number is defined, only the IP directed broadcast packets that match this access list are converted.

Defaults The conversion function is disabled.

Command Mode Interface configuration mode

Usage Guide An IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, a 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-1s), and then sends the packet to all hosts in the destination subnet as with link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a directed 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 will perform the conversion from directed broadcast to 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 the forwarding of directed broadcast packet on the FE port 0/1 of the device.

```
interface fastEthernet 0/1
ip directed-broadcast
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

ip addresss-pool local

Use this command to enable the IP address pool function. Use the no form of this command to disable the IP address pool function.

ip address-pool local

no ip address-pool local

Parameter Description

Parameter	Description
N/A	N/A

Defaults The IP address pool function is enabled.

Command Mode Global configuration mode

Usage Guide By default, the IP address pool function is enabled, the user can configure the IP address pool, and the PPP user can assign an IP address to the peer end from the IP address pool. Use the **no ip address-pool local** command to disable the IP address pool function and delete all IP address pools previously configured.

Configuration Examples The following example enables the IP address pool function.

```
ip address-pool local
```

Related Commands

Command	Description
ip local pool	Configures the IP address pool.

Platform Description This command is not supported on switches.

ip local pool

Use this command to specify an address pool for IP address assignment. Use the **no** form of this command to delete the specified IP address pool.

ip local pool *pool-name low-ip-address* [*high-ip-address*]

no ip local pool *pool-name* [*low-ip-address* [*high-ip-address*]]

Parameter Description

Parameter	Description
pool-name	Specifies the name of the local IP address pool. The default address pool is named **default**.
low-ip-address	The smallest IP address in the IP address pool.
high-ip-address	(Optional) The largest IP address in the IP address pool. If the largest one is not specified, only one address (low-ip-address) exists in the IP address pool.

Defaults No IP address pools are configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to create one or multiple IP address pools for PPP to assign IP addresses to connected users.

Configuration Examples The following example creates a local IP address pool named quark, with IP addresses ranging from 172.16.23.0 to 172.16.23.255.

```
ip local pool quark 172.16.23.0 172.16.23.255
```

Related Commands

Command	Description
ip address-pool local	Enables the IP address pool function.
peer default ip address	Assigns an IP address to the peer end.

Platform Description This command is not supported on switches.

clear arp-cache

Use this command to remove dynamic ARP mapping records from the ARP cache table in privileged mode.

clear arp-cache [**vrf** *vrf_name*] [*p* [*mask*]] | **interface** *interface-name*]

Parameter

Parameter	Description

Description

vrf *vrf_name*	Removes dynamic ARP entries of the specified VRF instance.
ip	Specifies the IP address so as to remove ARP entries of this IP address. If the *trusted* keyword is specified, trusted ARP entries are removed; otherwise, dynamic ARP entries are removed.
mask	Specifies the subnet mask so as to remove ARP entries of the specified subnet. The preceding IP address must be a subnet number. If the *trusted* keyword is specified, trusted ARP entries of the subnet are removed; otherwise, dynamic ARP entries of the subnet are removed.
interface *interface-name*	Removes dynamic ARP entries of the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to refresh an ARP cache table.


Caution

A Network Foundation Protection Policy (NFPP) device receives one ARP packet for every MAC or IP address per second by default. If the interval between twice ARP clearing is within 1 second, the second response packet will be filtered out and the ARP packet will fail to be parsed in a short time.

Configuration Examples The following example removes all dynamic ARP mapping records.

clear arp-cache

The following example removes the dynamic ARP entry 1.1.1.1.

```
clear arp-cache 1.1.1.1
```

The following example removes dynamic ARP table entries on interface SVI1.

```
clear arp-cache interface Vlan 1
```

Related Commands

Command	Description
arp	Adds a static mapping record to the ARP table.

Platform Description The parameter *trusted* is not supported by routers.

clear ip route

Use this command to remove the entire IP routing table or a particular routing record in the IP routing table in privileged EXEC mode.

clear ip route { ***** **|** *network* [*netmask*] }

Parameter Description

Parameter	Description
*	Removes all the routes.
network	The network or subnet address to be removed
netmask	(Optional) Network mask

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Once an invalid route is found in the routing table, you can immediately refresh the routing table to get the updated routes. Note that, however, refreshing the entire routing table will result in a temporary communication failure on the entire network.

Configuration Examples The following example refreshes only the route 192.168.12.0.

```
clear ip route 192.168.12.0
```

Related Commands

Command	Description
show ip route	Shows the IP routing table.

Platform Description This command is not supported on Layer 2 switches.

show arp

Use this command to show the ARP cache table

show arp [[**vrf** *vrf-name*] [**trusted**] *ip* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Shows ARP entries of the specified VRF instance.
trusted	Shows trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
ip	Shows the ARP entries of the specified IP address. If the *trusted* keyword is specified, only trusted ARP entries are shown; otherwise, non-trusted ARP entries are shown.
ip mask	Shows the ARP entries of the IP subnet. If the *trusted* keyword is specified, only trusted ARP entries are shown; otherwise, non-trusted ARP entries are shown.

static	Shows all the static ARP entries.
complete	Shows all the resolved dynamic ARP entries.
incomplete	Show alls the unresolved dynamic ARP entries.
mac-address	Shows the ARP entry with the specified MAC address.

Defaults N/A

Command Mode Priviledged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows 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
```

Field	Description
Protocol	Protocol of the network address,which is always set to **Internet**
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record in minutes If it is locally or statically configured, the value of the field is represented with “-”.
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, which is ARPA for Ethernet addresses
Interface	Interface associated with the IP address

The following example shows the output result of the **show arp 192.168.195.68** command.

```
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 example shows the output result of the show arp 192.168.195.0 255.255.255.0
command.
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 shows the output result of the show arp 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   VLAN 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported by routers or Layer 2 switches.

show arp counter

Use this command to show 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 Any mode

Usage Guide N/A

Configuration Examples The following example shows the output result of the **show arp counter** command:

```
Ruijie# show arp counter
The Arp Entry counter:0
The Unresolve Arp Entry:0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show arp timeout

Use this command to show the aging time of the dynamic ARP entry on an interface.

show arp timeout

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example shows the output result of the **show arp timeout** command:

```
Ruijie# show arp timeout
Interface             arp timeout(sec)
----------------------  ----------------
VLAN 1                3600
```

Related Commands	Command	Description
	N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

show ip arp

Use this command to show the ARP cache table in privileged EXEC mode.

show ip arp

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 shows the output result of the **show ip arp** command.

```
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
```

Field	Description
Protocol	Network address protocol, which is always set to **Internet**
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record in minutes If it is 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, which is **ARPA** for Ethernet addresses
Interface	Interface associated with the IP address

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

show ip interface

Use this command to show information about the IP status of an interface.

show ip interface [*interface-type interface-number* | **brief**]

Parameter Description

Parameter	Description
interface-type	Speciies the interface type.
interface-number	Specifies the interface number.
brief	Shows brief configuration information about the IP addresses of the layer-3 interface, including the interface primary IP address, secondary IP address, 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. An available interface means 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 direct route from the routing table.

If the interface is unavailable (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 interface-specific options.

Configuration Examples The following example shows the output result 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
```

Note:

Status: link status of the interface. The options include **up**, **down**, and **administratively down**. The link status of an interface will be **administratively down** if you run the **shutdown** command to forcibly shut down the interface.

Protocol: IPv4 protocol status of the interface.

The following example shows the output result 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
```

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:	Shows the interface type, such as broadcast or point-to-point.
IP interface MTU is:	Shows the MTU value of the interface.
IP address is:	Shows the IP address and mask of the interface.
IP address negotiate is:	Shows whether to obtain the IP address through negotiation.
Forward direct-broadcast is:	Shows whether to forward directed broadcast packets.
ICMP mask reply is:	Shows whether to send ICMP mask response messages.
Send ICMP redirect is:	Shows whether to send ICMP redirection messages.
Send ICMP unreachabled is:	Shows whether to send ICMP unreachable messages.
DHCP relay is:	Shows whether DHCP relay is enabled.
Fast switch is:	Shows whether the IP fast switching function is enabled.
Route horizontal-split is:	Shows whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Shows the helper IP address.
Proxy ARP is:	Shows whether the proxy ARP is enabled.
ARP packet input number: 0 Request	Shows the total number of ARP packets received on the interface, including: ARP request packets

packet: 0 Reply packet: 0 Unknown packet: 0	ARP reply packets Unknown packets
TTL invalid packet number:	Shows the number of packets with invalid TTL.
ICMP packet input number: 0 Echo request: 0 Echo reply: 0 Unreachable: 0 Source quench: 0 Routing redirect: 0	Shows the total number of ICMP packets received on the interface, including: Echo request packets Echo reply packets Unreachable packets Source quench packets Routing redirection packets
Outgoing access list is	Shows whether an outgoing access list has been configured for an interface.
Inbound access list is	Shows whether an incoming access list has been configured for an interface.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip packet statistics

Use this command to show the statistics of IP packets.

show ip packet statistics [**total** | *interface-name*]

Parameter Description

Parameter	Description
total	Shows the total statistics of all interfaces.
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie#show ip packet statistics
Total
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50,Broadcast:0

VLAN 1
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50,Broadcast:0
```

Related Commands

Command	Description
ip default-gateway	Configures the default gateway, which is only supported on Layer 2 switches.

Platform Description N/A

show ip pool

Use this command to display an IP address pool of the system.

show ip pool [*pool-name*]

Parameter Description

Parameter	Description
pool-name	Address pool name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows the output result of the **show ip pool** command.

```
Ruijie#show ip pool
Pool       Begin         End               Free   In use
aaa       1.1.1.1        1.1.1.200           200       0
ccc       2.2.2.2        2.2.2.211           210       0
```

Related Commands

Command	Description
ip local pool	Configures the IP address pool.

Platform Description This command is not supported on switches.

show ip redirects

Use this command to show the default gateway.

show ip redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is supported on L2 switches only.

Configuration Examples The following example shows the output result of the **show ip redirects** command.

```
Ruijie# show ip redirects
Default Gateway: 192.168.195.1
```

Related Commands

Command	Description
ip default-gateway	Configures the default gateway, which is only supported on Layer 2 switches.

Platform Description N/A

ip mask-reply

Use this command to configure the RGOS software to respond to the ICMP mask request and send an ICMP response message in interface configuration mode. Use the **no** form of this command to disable the sending of the ICMP mask response message.

ip mask-reply

no ip mask-reply

Parameter Description

Parameter	Description
N/A	N/A

Defaults No ICMP mask response message is sent.

Command Mode Interface configuration mode

Usage Guide Sometimes a network device needs to know 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 return a mask response message.

Configuration Examples The following example sets the FE interface 0/1 of a device to respond to the ICMP mask request message.

```
interface fastEthernet 0/1
ip mask-reply
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for IP packets in interface configuration mode. Use the **no** form of this command to restore the default settings.

ip mtu *bytes*

no ip mtu

Parameter Description

Parameter	Description
bytes	Maximum transmission unit of IP packets ranging from 68 to 1500

	bytes

Defaults The MTU is the same as the MTU value configured by the interface command **mtu**.

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 MTU value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

Configuration Examples The following example sets the IP MTU value of the FE interface 0/1 to 512 bytes.

```
interface fastEthernet 0/1
ip mtu 512
```

Related Commands

Command	Description
mtu	Sets the MTU value of an interface.

Platform Description This command is not supported on Layer 2 switches.

ip redirects

Use this command to allow the RGOS software to send an ICMP redirection message in interface configuration mode. Use the **no** form of this command to disable the ICMP redirection function.
ip redirects
no ip redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults The ICMP redirection function is enabled.

Command Mode Interface configuration mode

Usage Guide When the route is not optimal, it may cause the device to receive packets through one interface and send it though the same interface. If the device sends the packet from the same 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 optimal path.
The RGOS software enables ICMP redirection by default.

Configuration Examples The following example disables ICMP redirection on the FE interface 0/1.

```
interface fastEthernet 0/1
no ip redirects
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

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 the source route information processing function.
ip source-route
no ip source-route

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is enabled.

Command Mode Global configuration mode

Usage Guide RGOS supports IP source routes. 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 error message will be sent to the data source, and then this packet is discarded.
The RGOS software supports IP source routes by default.

Configuration Examples The following example disables the IP source route feature.

```
no ip source-route
```

Related Commands

Command	Description

N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

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 The function is enabled.

Command Mode Interface configuration mode

Usage Guide RGOS software will send an ICMP destination unreachable message if it receives a unicast message in which the destination address is itself and cannot process the upper protocol of this message.
RGOS software will send an ICMP host unreachable message to the data source if it cannot forward a message due to no routing.
This command influences all ICMP destination unreachable messages.

Configuration Examples The following example disables the sending of ICMP destination unreachable messages on the FE interface 0/1.

```
interface fastEthernet 0/1
no ip unreachables
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is not supported on Layer 2 switches.

VRF Commands

address-family

Use this command to configure an IPv4 address family or IPv6 address family for a multiprotocol VRF.

address-family { **ipv4 | ipv6** }

no address-family { **ipv4 | ipv6** }

Parameter Description

Parameter	Description
N/A	N/A

Defaults No IPv4 address family or IPv6 address family is configured for a multiprotocol VRF.

Command Mode VRF configuration mode

Usage Guide When an IPv4 address family is configured for a multiprotocol VRF, IPv4 is enabled; when an IPv6 address family is configured for a multiprotocol VRF, IPv6 is enabled.

Configuration Examples The following example defines a multiprotocol VRF named *vrf1* and configures an IPv4 address family for this VRF.

```
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

description

Use this command to configure the VRF description.

description *string*

no description

Parameter Description

Parameter	Description
string	Character string, with the maximum length of 244 characters

Defaults N/A

Command Mode VRF configuration mode

Usage Guide N/A

Configuration Examples The following example defines a single-protocol IPv4 VRF named *vrf1* and sets the description to vpn-a.

```
Ruijie(config)#ip vrf definition vrf1
Ruijie(config-vrf)#description vpn-a
```

The following example defines a multiprotocol VRF named *vrf2* and sets the descriptions 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

exit-address-family

Use this command to exit the 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 named *vrf1* and configures an IPv4 address family for it.

```
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 or IPv6 address family for a multiprotocol VRF.
vrf definition	Defines a multiprotocol VRF.

Platform Description

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, which is a string of at most 31 characters

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to create a single-protocol IPv4 VRF.

Configuration Examples

```
Ruijie# ip vrf redvrf
```

Related Commands

Command	Description
RGOS10.1	RGOS10.1 and later versions

Platform Description N/A

ip vrf forwarding

Use this command to add an interface or sub-interface to a VRF. Use the **no** form of this command to remove an interface or sub-interface from 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 An interface does not belong to any VRF.

Command Mode Interface configuration mode

Usage Guide If the IPv6 function does not need to be enabled on an interface, you can bind the interface to a single-protocol IPv4 VRF.

If you bind an interface on a device that supports VRFs to a single-protocol IPv4 VRF and enables the IPv6 protocol on the interface, the device cannot forward IPv6 packets received on the interface. Therefore, it is recommended that you use the **vrf forwarding** command to bind an interface to a multi-protocol VRF, if you want to bind the interface to a VRF and enable the IPv6 protocol on the interface at the same time.

Configuration Examples

```
Ruijie(config-if)# ip vrf forwarding redvrf
```

Related Commands

Command	Description
RGOS10.1	RGOS10.1 and later versions

Platform Description N/A

ip vrf receive

Use this command to import the host and direct-connected routes of one interface into the specifed VRF routing table. Use the **no** form of this command to remove the imported host and direct-connetced routes from the VRF routing table.

ip vrf receive *vrf-name*

no ip vrf receive *vrf-name*

Parameter

Parameter	Description

Description

vrf-name	Name of the VRF that the host and direct-connected routes are imported into. It can be a single-protocol IPv4 VRF instead of a multiprotocol VRF.

Defaults The host and direct-connected routes of an interface are not imported into other VRFs by default.

Command Mode Interface configuration mode

Usage Guide Currently, the **ip vrf receive** command supports VRF routing based on PBR. This command is used to import the host routes with the master and slave addresses and direct-connected routes of this interface into the specified VRF routing table. You need to execute this command multiple times to import the host and direct-connected routes into multiple VRF routing tables. Unlike the **ip vrf forwarding** command, which does not bind the interface to a VRF, this interface still belongs to the global VRF.

On one interface, the **ip vrf forwarding** and **ip vrf receive** commands are mutually exclusive, the **vrf forwarding** and **ip vrf receive** are mutually exclusive. If one of them has been configured, when configuring the other one, failure information is returned.

If the **ip vrf forwarding** command is configured before the **ip vrf receive** command, the following prompt is returned:% Cannot configure 'ip vrf receive' if interface is under a VRF

If the **ip vrf receive** command is configured before the **ip vrf forwarding** command, the following prompt is returned:% Cannot bind interface to a VRF if it has configed 'ip vrf receive'

Configuration Examples

```
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 single-protocol IPv4 VRF.
set vrf	Sets a VRF intance in route map configuration

	mode.

Platform Description

vrf definition

Use this command to create a multiprotocol VRF. Use the **no** form of this command to delte the multiprotocol VRF instanc.

vrf definition *vrf-name*

no vrf definition ***vrf-name***

Parameter Description

Parameter	Description
vrf-name	VRF name supporting up to 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 creates a multiprotocol VRF named *vrf1*.

```
Ruijie(config)#vrf definition vrf1
Ruijie(config-vrf)#
```

Related Commands

Command	Description
description	Configures the description.
address-family	Configures an IPv4 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

vrf forwarding

Use this command to bind a network interface to a multiprotocol VRF. Use the **no** form of this command to cancel the binding.

vrf forwarding *vrf-name*

no 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, the IPv4 addresses and VRRP IPv4 addresses of all network interfaces bound to the VRF as well as the IPv4 static routes whose routing VRF or next-hop VRF is the VRF will be deleted. Likewise, if you delete a multiprotocol VRF's IPv6 address family, the IPv4 addresses and VRRP IPv6 addresses of all network interfaces bound to the VRF will be deleted, IPv6 will be disabled on the interfaces, and the IPv6 static routes whose routing VRF or next-hop VRF is that VRF will be deleted.

Configuration Examples The following example binds the interface VLAN 1 to a multiprotocol VRF named *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 Instance.

Platform Description

vrf receive

Use this command to add the local host route and direct route with the interface's IPv4/v6 address to the routing table of the specified VRF Instance. Use the **no** form of this command to delete the configuration.

vrf receive *vrf-name*

no 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 a 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 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 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 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 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 or IPv6 address family for a multiprotocol VRF.
set vrf	Configures a VRF in route map configuration mode.

Platform Description

show ip vrf

Use this command to show VRF information.

show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]

Parameter Description

Parameter	Description
brief	(Optional) Shows VRF information and related interface information in brief.
detail	(Optional) Shows VRF information and related interface information in detail.
interfaces	(Optional) Shows VRF information and related interface information in detail.

vrf-name	(Optional) Specifies the name of the VRF.

Defaults All VRF information is displayed in brief if no parameter is specified.

Command Mode Privileged EXEC mode

Usage Guide Use this command to show VRF information, which can be divided into two levels:

- Use the keyword **brief** to show information in brief.
- Use the keyword **detail** to show information in detail.
- Use the keyword **interfaces** to show a VRF's interface information.

Configuration Examples

```
Ruijie# show ip vrf redvrf
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show vrf

Use the following command to show the brief information of a VRF, which can be a single-protocol IPv4 VRF or a multiprotocol VRF:

show vrf [**brief**] [*vrf-name*]

Use the following command to show the brief information of a VRF configured with an IPv4 address family, which can be a single-protocol IPv4 VRF:

show vrf ipv4 [*vrf-name*]

Use the following command to show the brief information of a VRF configured with an IPv6 address family:

show vrf ipv6 [*vrf-name*]

Use the following command to show the detailed information of a VRF, which can be a single-protocol IPv4 VRF or a multiprotocol VRF:

show vrf detail [*vrf-name*]

Parameter Description

Parameter	Description
vrf-name	Name of the VRF

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration Examples The following example shows the brief information of all VRFs.

```
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
```

Related Commands

Command	Description
ip vrf	Defines a single-protocol IPv4 VRF.
vrf definition	Defines a multiprotocol VRF.

Platform Description

IPv4 REF Commands

ip ref load-sharing {original | packet}

Use this command to configure the IPV4 REF load balancing algorithm to be destination IP address plus source IP address. The no form of this command can recover the default destination IP balancing algorithm. If one IP/MASK maps multiple next hops, this command can set the routing strategy for forwarding packets to realize load balancing. The two strategies that have been realized are as follows:

Balance the load according to the destination addresses of IP packets, and process the destination IP addresses of the packets through the hashing algorithm. The path with greater weight is more probable to be selected. This strategy is adopted by default.

Balance the load according to the destination and source IP addresses of IP packets and process the destination and source IP addresses of the packets with the hashing algorithm. The path with greater weight is more probable to be selected.

Balance the load according to packets polling. Each packet takes turn to select the path and all paths can be selected.

ip ref load-sharing original

[no] ip ref load-sharing {original | packet}

Parameter Description

Parameter	Description
original	Performs the load balancing according to the destination IP address plus source IP address
packet	Performs the load balancing according to packet polling

Defaults N/A

Command Mode Global configuration mode

Usage Guide The REF software on the router is used for data forwarding. It also supports three load balancing algorithms, The first one is destination IP address load balancing algorithm; the second one is destination IP address plus source IP address load balancing algorithm; and the third one is packet polling. When a IP packet is forwarded through multiple paths, and the former algorithm is set currently, REF can match one of the paths based on the destination IP address of the packet. By default, the destination IP load balancing algorithm is used.

Configuration Examples Example 1: The following example configure the balancing routing algorithm of source IP addresses plus destination IP addresses.

```
Ruijie(config)# ip ref load-sharing original
```

Example 2:The following example configures the balancing routing basing on packets polling

```
Ruijie(config)# ip ref load-sharing packet
```

Example 3: The following example uses the balancing routing algorithm based on the destination IP addresses of packets.

```
Ruijie(config)# no ip ref load-sharing original
```

Related Commands

Command	Description
N/A	N/A

Platform Description

ref parameter

Configure the performance parameters of REF.

ref parameter *{ 20-95 }* [*200-1000*]

Parameter Description

Parameter	Description
The first mandatory parameter is within the scope of { 20-95 }.	Indicates the percentage of cpu0 occupied by REF.
The second optional parameter is within the scope of { 200-1000 }.	Indicates the cycle of computing the percentage of cpu0 occupied by REF is 200μs by default.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command can be used to adjust the percentage of cpu0 occupied by REF.

Configuration Examples Example 1: Configure that the percentage of cpu0 occupied by REF is 50%, and the computing cycle is 500μs.

```
Ruijie(config)#ref parameter 50 500
```

Example 2: Configure that the percentage of cpu0 occupied by REF is 80%, and the computing cycle is the currently configured cycle.

```
Ruijie(config)#ref parameter 80
```

Example 3: Configure that the percentage of cpu0 occupied by REF is 1 by default in the system.

```
Ruijie(config)#no ref parameter
```

Example 4: Configure that the percentage of cpu0 occupied by REF is 2 by default in the system.

```
Ruijie(config)#default ref parameter
```

Related Commands

Command	Description
N/A	N/A

Platform Description

show ip ref adjacency

Use this command to display a special adjacent node or all the current adjacent nodes.

show ip ref adjacency [**glean | local | punt |** *ip* **| interface** *interface_type interface_number* **| statistic**]

Parameter Description

Parameter	Description
glean	Gleans the adjacent nodes.
local	Local adjacent nodes
punt	Punt adjacent nodes
ip	IP of the next hop
interface_type	Specifies the type of interface
interface_number	Specifies the number of interface
statistic	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display the adjacent table in the current REF module. The table displays the gleaned adjacency, local adjacency, IP adjacency, interface-related adjacency and all the adjacent node information.

Configuration Examples Example 1: Display all the adjacent information in the adjacent table.

```
Ruijie#show ip ref adjacency
id state type rfct chg  ip   interface     linklayer(header data)
2  unresolved punt    1    0   0.0.0.0
1  unresolve   mcast    1   0   224.0.0.0
9  resolved   forward 1  0   192.168.50.78   FastEthernet 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  FastEthernet 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        FastEthernet 0/0
4 unresolved local  3  0   0.0.0.0        Local 0
```

Field	Description
id	Adjacent identity
state	Adjacent state unresolved resolved
type	Adjacent type local: local adjacency forward:forwarding adjacency drop:dropping adjacency glean:gleaning adjacency
rfct	Count of the used adjacency
chg	Whether the adjacency is in the changing link?
l2addr	L2 header
interface	Egress

Related Commands

Command	Description
show ip ref route	Displays all routing information in the current REF module.

Platform Description

show ip ref exact-route

Use this command to display the accurate forwarding path of an IP packet.

show ip ref exact-route [**vrf** *vrf_name*] *source-ipaddress dest_ipaddress*

Parameter Description

Parameter	Description
vrf	Virtual routing forwarding
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 Example 1:

```
Ruijie#show ip ref exact-route 192.168.50.122 192.168.50.123
192.168.50.122 --> 192.168.50.123 (vrf global):
id      state          type      rfct  chg  ip                    interface
linklayer(header data)
6    unresolve   glean   1    0   0.0.0.0       FastEthernet 0/0
```

Related Commands

Command	Description
show ip ref route	Displays all routing information in the current REF module.

Platform Description

show ip ref packet-statistic

Use this command to display current packet statistics of REF. This command is as follows:
show ip ref packet-statistic [**clear**]

Parameter Description

Parameter	Description
clear	Clears the statistics.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display current packet statistics of REF.

Configuration Examples Example 1:

```
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

show ip ref route

Use this command to display all the routing information on the current REF module.

show ip ref route [**vrf** *vrf_name*] [**default** | (*ip mask*) | **statistic**]

Parameter Description

Parameter	Description
vrf	Virtual routing forwarding
default	Specifies default route.
ip	Specifies the destination IP address of route.
mask	Specifies the routing mask.
statistic	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide 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 Example 1: Display all the routing information in the 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

TCP Commands

ip tcp adjust-mss

Use this command to change the MSS option value of SYN packets sent and received on an interface. Use the **no** form of this command to remove the configuration.

ip tcp adjust-mss *max-segment-size*

no ip tcp adjust-mss

Parameter Description

Parameter	Description
max-segment-size	Maximum segment size in the range from 500 to 1460 bytes

Defaults The MSS option value of SYN packets is not changed.

Command Mode Interface configuration mode

Usage Guide MSS refers to the maximum size of the payload of a TCP packet.

The TCP Path MTU (PMTU) is implemented as per RFC1191. This feature can improve the network bandwidth utilization ratio. When the user uses TCP to transmit mass data, this feature can substantially enhance the transmission performance.

When the client initiates a TCP connection, it negotiates the maximum payload of TCP packets through the MSS option field of the TCP SYN packet. The MSS value of the client's SYN packet implies the maximum payload of TCP packets sent by the server, and vice versa.

Configuring this command on the interface will change the MSS option of SYN packets received or sent by the interface to the MSS value configured on the interface. If the MSS is configured on both the inbound interface and the outbound interface of the SYN packet, the smaller of the two applies. It is recommended that you configure the same value on the inbound interface and outbound interface.

This command actually changes the SYN packet exchanged during TCP connection establishment. For some versions, this command may also change the SYN+ACK packet.

This command takes effect on the subsequent TCP connections to be established instead of established TCP connections.

This command only applies to IPv4 TCP.

Configuration Examples

```
Ruijie(config-if)# ip tcp adjust-mss 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported by RGOS 10.4 and later versions as well as 10.3(5b6) and 10.3(5b8).

ip tcp mss

Use this command to configure the upper limit of the MSS value. Use the **no** form of this command to remove the configuration.

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 upper limit is not set by default.

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.

Configuration Examples

```
Ruijie(config)# ip tcp mss 1300
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported by RGOS 10.3 and later versions.

ip tcp not-send-rst

Use this command to prohibit sending the reset packet when a port-unreachable packet is received. Use the **no** form of this command to remove the configuration.

ip tcp not-send-rst

no ip tcp not-send-rst

Parameter Description

Parameter	Description

N/A	N/A

Defaults The reset packet is sent when a port-unreachable packet is received.

Command Mode Global configuration mode

Usage Guide When the TCP module distributes TCP packets, if the TCP connection to which such packets belong cannot be found, a reset packet will be returned to the peer end to terminate the TCP connection. The attacker may initiate attacks by sending a large number of port-unreachable TCP packets. You can use this command to prohibit sending the reset packet when a port-unreachable packet is received.

Configuration Examples

```
Ruijie(config)# ip tcp not-send-rst
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported by RGOS 10.3 and later versions.

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 disable this function.

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 The PMTU discovery function is disabled.

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 is valid for both IPv4 and IPv6 TCP.

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

```
Ruijie(config)# ip tcp path-mtu-discovery
```

Related Commands

Command	Description
show tcp pmtu	Shows the PMTU value for the TCP connection.

Platform Description This command is supported by RGOS 10.3 and later versions.

ip tcp syntime-out

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 value.

ip tcp syntime-out *seconds*

no ip tcp syntime-out

Parameter Description

Parameter	Description
seconds	Timeout value for SYN packets in the range from 5 to 300 seconds. The default value is 20.

Defaults 20 seconds

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.

Configuration Examples

```
Ruijie(config)# ip tcp syntime-out 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported by RGOS 10.3 and later versions.

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 value.

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 0 to 65535 bytes. The default value is 4096.

Defaults The size of receiving buffer and sending buffer is 4096 bytes.

Command Mode Global configuration mode

Usage Guide The TCP receiving buffer is used to buffer the data received from the peer end. These data will be subsequently read by application programs. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For connections involving a large bandwidth and mass data, increasing the size of receiving buffer will remarkably improve TCP transmission performance.

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.

Configuration Examples

```
Ruijie(config)# ip tcp window-size 16386
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported by RGOS 10.3 and later versions.

show tcp connect

Use this command to display basic information about the current TCP connections.

show tcp connect

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie#sh tcp connect
tcp connect status:
TCB       Local Address    Foreign Address         State
cf25000    0.0.0.0.2650     0.0.0.0.0              LISTEN
c441000    0.0.0.0.23       0.0.0.0.0              LISTEN
c441800    1.1.1.1.23       1.1.1.2.64201           ESTABLISHED
c444cc0    ::.23           ::.0                   LISTEN
c429980    3000::1.23       3000::2.64236           ESTABLISHED
```

Field	Description
TCB	The control block's location in the current memory
Local Address	Th 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.

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported by RGOS 10.3 and later versions.

show tcp pmtu

Use this command to display information about TCP PMTU.

show tcp pmtu

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# show tcp pmtu
No.      Local Address          Foreign Address       PMTU
[1]      2002::1.18946          2002::2.23           1440
[2]      192.168.195.212.23     192.168.195.112.13560  1440
```

Field	Description
No.	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 This command is supported by RGOS 10.3 and later versions.

show tcp port

Use this command to show information about the current TCP port.

show tcp port

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie#sh tcp port
tcp port status:
Tcpv4 listen on 2650 have connections:
TCB       Foreign Address                      Port    State
Tcpv4 listen on 2650 have total 0 connections.
Tcpv4 listen on 23 have connections:
TCB       Foreign Address                      Port    State
c340800   1.1.1.2                             64571   ESTABLISHED
Tcpv4 listen on 23 have total 1 connections.
Tcpv6 listen on 23 have connections:
```

```
TCB       Foreign Address                          Port     State
c429980    3000::2                                64572    ESTABLISHED
```

Tcpv6 listen on 23 have total 1 connections.

Field	Description
TCB	The control block's location in the current memory
Foreign Address	Remote address
Port	Remote port number
State	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 This command is supported by RGOS 10.3 and later versions.

Application Protocol Configuration Commands

17. URL-Group Commands
18. URL-LIB Commands

DNS Module Commands

ip domain-lookup

Use this command to enable the Domain Name System (DNS) for domain name resolution. Use the **no** form of this command to disable DNS domain name resolution.

ip domain-lookup

no ip domain-lookup

Parameter Description

Parameter	Description
N/A	N/A

Defaults Domain name resolution is enabled by default.

Command Mode Global configuration mode

Usage Guide This command enables the domain name resolution function.

Configuration Examples The following example enables DNS domain name resolution.

```
Ruijie(config)# ip domain-lookup
```

Related Commands

Command	Description
show hosts	Shows the DNS related configuration information.

Platform Description N/A

ip name-server

Use this command to configure the IP/IPv6 address of the domain name server. Use the **no** form of this command to delete the configured DNS server.

ip name-server { *ip-address* | *ipv6-address* }

no ip name-server [*ip-address* | *ipv6-address*]

Parameter Description

Parameter	Description
ip-address	IP address of the DNS server

ipv6-address	IPv6 address of the DNS server

Defaults No DNS is configured by default.

Command Mode Global configuration mode

Usage Guide Add the IP/IPv6 address of the DNS server. Once this command is executed, the device will add a DNS. When the device cannot obtain the domain name from a DNS, it will attempt to send the DNS request to subsequent servers until it receives a response.
Up to six DNS servers are supported. You can delete a DNS with the *ip-address* option or all the DNS servers.

Configuration Examples
```
Ruijie(config)# ip name-server 192.168.5.134
```

Related Commands

Command	Description
show hosts	Shows the DNS related configuration information.

Platform Description N/A

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	Host name of the device
ipv6-address	IPv6 address of the device

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
```
Ruijie(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

Examples

Related Commands

Command	Description
show hosts	Shows the DNS related configuration information.

Platform Description N/A

ip host

Use this command to configure the mapping of the host name and the IP address by manual. 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	Host name of the device
ip-address	IP address of the device

Defaults N/A

Command Mode Global configuration mode

Usage Guide To delete the host list, use the **no ip host** *host-name ip-address* command.

Configuration Examples

```
Ruijie(config)# ip host switch 192.168.5.243
```

Related Commands

Command	Description
show hosts	Shows the DNS related configuration information.

Platform Description N/A

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	Host name of the device
ipv6-address	IPv6 address of the device

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

```
Ruijie(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

Related Commands

Command	Description
show hosts	Shows the DNS related configuration information.

Platform Description N/A

clear host

Use this command to clear the host name-IP address buffer table in privileged user mode.

clear host [*host-name*]

Parameter Description

Parameter	Description
host-name	Deletes the specified dynamically learned host. The asterisk (*) denotes to clear all the dynamically learned host names.

Defaults N/A

Command Mode Privileged user mode

Usage Guide You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** or **ipv6 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 example deletes the dynamically learned mapping records from the host name-IP address buffer table.

clear host *

Related Commands

Command	Description
show hosts	Shows the host name buffer table.

Platform Description N/A

show hosts

Use this command to show DNS configuration information.

show hosts

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide Shows the DNS related configuration information.

Configuration Examples

```
Ruijie# show hosts
Name servers are:
static
host                type          address
switch              static        192.168.5.243
www.ruijie.com      dynamic       192.168.5.123
```

Related Commands

Command	Description
ip host	Configures the host name and IP address mapping manually.
ipv6 host	Configures the host name and IPv6 address mapping manually.
ip name-server	Configures the DNS server.

Platform N/A

Description

DDNS Commands

peanut username

Use this command to configure an Oray account and password. Use the **no** form of this command to remove the configuration.

peanut username *name* **password** *password*

no peanut username *name* **password** *password*

Description

Parameter	Description
name	Indicates the Oray username.
password	Indicates the Oray password.

Default Configuration

Oray client is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures an Oray account.

```
Ruijie#configure
Enter configuration commands, one per line.   End with CNTL/Z.
Ruijie(config)#peanut username ruijie password ruijie
```

Related Commands

Command	Description
show hosts	Displays the DNS configuration.

Platform Description

N/A

show peanutinfo

Use this command to display the Oray status of the device.

show peanutinfo

Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the Oray configuration, including the Oray status, Oray account and Oray password.

Configuration Examples

```
Ruijie#show peanutinfo
peanut state: linking
peanut username:ruijie
peanut password:ruijie
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

DHCP Commands

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 remove the network segment range.

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 No network segment range is configured for the associated class by default. In this case, the network segment range of the address pool is used,.

Command Mode Address pool class configuration mode

Usage Guide Each class corresponds to one network segment range, which must be from the low address to the high address. Multiple classes can have duplicated network segment ranges. If the class associated with the address pool is specified without the corresponding network segment range configured, the default network segment range of this class is same as that of the address pool where this class resides.

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 DHCP address pool configuration mode.
class	Configures the class associated with the DHCP address pool and enters address pool class configuration mode.

Platform Description N/A

bootfile

Use this command to define the startup mapping file name of the DHCP client in DHCP address pool configuration mode. Use the **no** form of this command to remove the definition.

bootfile *file-name*

no 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 the configuration file during 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 Trivial File Transfer Protocol (TFTP). Other servers are defined by the **next-server** command.

Configuration Examples The following example defines **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 enters DHCP address pool configuration mode.
next-server	Configures the next server IP address of the DHCP client startup process.

Platform Description N/A

class

Use this command to configure the associated class in the DHCP address pool. Use the **no** form of this command to delete the associated class.

class *class-name*

no class

Parameter Description

Parameter	Description
class-name	Class name, which can be a character string or number such as **myclass** or 1.

Defaults No class is associated with the address pool by default.

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. One DHCP address pool can map to multiple classes, and different classes can specify different network segment ranges.
During the address assignment, firstly, ensure the assignable address pool based on the network segment where the client resides, then locate the class according to the Option82 information, and assign the IP address from the network segment range of the class. If one request packet matches multiple classes in the address pool, perform the address assignment according to the priority order configured for the class in the address pool. If addresses assigned to this class have been to the upper limit, continue to assign the address from the next class. 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 range of the class is same as that of the address pool where the class resides.

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 DHCP address pool configuration mode.

Platform Description N/A

client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hexadecimal separated by dot) in DHCP address pool configuration mode. Use the **no** form of this command to delete the client ID.
client-identifier *unique-identifier*
no client-identifier

Parameter Description

Parameter	Description
unique-identifier	DHCP client ID indicated in hexadecimal 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 then their hardware addresses. The client ID consists of the media type, MAC addresses and interface name. For example, 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 hexadecimal code of GigabitEthernet0/1. For the definition of the media code, see the section "Address Resolution Protocol Parameters" in the *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.

```
Ruijie(dhcp-config)# 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 DHCP address pool configuration mode.

Platform Description N/A

client-name

Use this command to define the name of the DHCP client in DHPC address pool configuration mode.
Use the **no** form of this command to delete the name of the DHCP client.
client-name *client-name*
no client-name

Parameter Description

Parameter	Description
client-name	Name of DHCP client, which is a set of standard-based ASCII characters. The name should not include the suffix domain name. For example, 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.

```
Ruijie(dhcp-config)# 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 DHCP address pool configuration mode.

Platform Description N/A

default-router

Use this command to define the default gateway of the DHCP client in DHPC address pool configuration mode. Use the **no** form of this command to delete the definition of the default gateway.

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 eight 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 at least one gateway address for the client, 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.

```
Ruijie(dhcp-config)# default-router 192.168.12.1
```

Related

Command	Description

Commands		
	ip dhcp pool	Defines the name of the DHCP address pool and enters DHCP address pool configuration mode.

Platform Description N/A

dns-server

Use this command to define the Domain Name System (DNS) server of the DHCP client in DHPC address pool configuration mode. Use the **no** form of this command to delete the definition of the DNS server.

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 eight DNS servers can be configured.

Defaults No DNS server is defined by default.

Command Mode DHCP address pool configuration mode

Usage Guide When multiple DNS servers are 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.

Configuration Examples The following example specifies the DNS server 192.168.12.3 for the DHCP client.

```
Ruijie(dhcp-config)# 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 DHCP address pool configuration mode.

Platform Description N/A

domain-name

Use this command to define the suffix domain name of the DHCP client in DHPC address pool configuration mode. Use the **no** form of this command to delete the suffix domain name.

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 is defined 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.

```
Ruijie(dhcp-config)# 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 enters DHCP address pool configuration mode.

Platform Description N/A

hardware-address

Use this command to define the hardware address of the DHCP client in DHPC address pool configuration mode. Use the **no** form of this command to delete the definition of the hardware address.

hardware-address *hardware-address* [*type*]

no hardware-address

Parameter Description

Parameter	Description
hardware-address	Defines the hardware address of the DHCP client.
type	Uses the string definition or digits definition to indicate the hardware platform protocol of the DHCP client,: String options: Ethernet

	ieee802 Digits options: 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 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.

```
Ruijie(dhcp-config)# hardware-address 00d0.f838.bf3d
```

Related Commands

Command	Description
client-identifier	Defines the unique ID of the DHCP client (Indicated in hexadecimal 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 enters DHCP address pool configuration mode.

Platform Description N/A

host

Use this command to define the IP address and network mask of the DHCP client host in DHCP address pool configuration mode. Use the **no** form of this command to delete the definition of the IP address and network mask for the DHCP client.

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 by default.

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.

```
Ruijie(dhcp-config)# 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 hexadecimal 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 DHCP address pool configuration mode.

Platform Description N/A

ip address dhcp

Use this command to enable the Ethernet interface or the Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC) and Frame Relay (FR) encapsulated interface to obtain the IP address information through DHCP. The **ip address dhcp** command is configured on the common DHCP clients, while the **ip address dhcp 6rd** command is configured on the DHCP clients that support automatic 6RD configuration. Use the **no** form of this command to remove this configuration.

ip address dhcp [**6rd**]

no ip address dhcp

Parameter Description

Parameter	Description
6rd	Applies for 6RD parameter configuration while requesting the DHCP IP address.

Defaults The interface cannot obtain the IP 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 to provide information about five configuration parameters: 1) DHCP option 1, indicates the client subnet mask; 2) DHCP option 3, indicates the same as the gateway information of the same subnet; 3) DHCP option 6, indicates the DNS server information; 4) DHCP option 15, indicates the host suffix domain name; 5) DHCP option 44, indicates 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, Ruijie DHCP server supports this function.

Configuration Examples The following example makes the FastEthernet 0 port obtain the IP address automatically.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-FastEthernet 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 DHCP address pool configuration mode.

Platform Description N/A

ip dhcp class

Use this command to define a class and enter global class configuration mode. Use the **no** form of this command to delete the global class.

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 The class is not configured by default.

Command Mode Global configuration mode

Usage Guide After executing this command, the system enters global class configuration mode which is shown as “Ruijie (config-dhcp-class)**#**”. In this configuration mode, you 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

ip dhcp database write-delay

Use this command to configure the function of writing the DHCP lease data-binding information into the FLASH timely in global configuration mode. Use the **no** form of this command to disable the function of writing timely.

ip dhcp database write-delay *time*

no ip dhcp database write-delay

Parameter Description

Parameter	Description
time	Interval at which the system writes the DHCP lease binding database information into the flash

Defaults This command is disabled by default.

Command Mode Global configuration mode

Usage Guide By configuring this command, you can write the information of DHCP lease binding database into the FLASH files to prevent the loss of user information after restarting the device.

Configuration Examples The following example configures that the switch writes the information into FLASH every 3600 seconds.

```
Ruijie(config)# ip dhcp database write-delay 3600
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp database write-to-flash

Use this command to write the information of DHCP lease binding data into FLASH files in real-time in global configuration mode.

ip dhcp database write-to-flash

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide By configuring this command, you can write the information of DHCP lease binding database into the FLASH files in real-time.

Configuration Examples The following example writes the binding database information into FLASH manually.

```
Ruijie(config)# ip dhcp database write-to-flash
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp excluded-address

Use this command to define some IP addresses and prevent the DHCP server from assigning them to the DHCP client in global configuration mode. Use the **no** form of this command to cancel this definition.

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 no excluded IP address is 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 the DHCP from assigning these addresses 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 The following example configures that the DHCP server will not assign the IP addresses within 192.168.12.100 to 150.

```
Ruijie(config)# 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 DHCP address pool configuration mode.

network (DHCP)	Defines the network number and network mask of the DHCP address pool.

Platform Description N/A

ip dhcp ping packets

Use this command to configure the times of pinging the IP address when the DHCP server detects the address conflict in global configuration mode. Use the **no** form of this command to restore the default configuration

ip dhcp ping packets [*number*]

no ip dhcp ping packets

Parameter Description

Parameter	Description
number	(Optional) Number of packets in the range from 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 to **3**.

```
Ruijie(config)# ip dhcp ping packets 3
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears the DHCP history conflict record.
ip dhcp ping packets	Configures the timeout that the DHCP server waits for the ping response. If all the ping packets are not responded within the specified time, this IP address can be assigned. Otherwise, it will record the address conflict.
show ip dhcp conflict	Shows the DHCP server detects address conflict when it assigns an IP address.

Platform Description N/A

ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for a response when it uses the ping operation to detect the address conflict in global configuration mode. Use the **no** form of this command to restore it to the default configuration.

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 timeout is 500 seconds by default.

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 that the waiting time of the ping response packet is 600ms.

Ruijie(config)# **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 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	Shows the address conflict the DHCP server detects when it assigns an IP address.

Platform Description N/A

ip dhcp pool

Use this command to define a name of the DHCP address pool and enter DHCP address pool configuration mode in global configuration mode. Use the **no** form of this command to delete the DHCP address pool.

ip dhcp pool *pool-name*

no ip dhcp pool *pool-name*

Parameter Description

Parameter	Description
pool-name	String of characters and positive integers, for

	example, mypool or 1.

Defaults No DHCP address pool is defined by default.

Command Mode Global configuration mode

Usage Guide Execute the command to enter DHCP address pool configuration mode, which is shown as:
Ruijie(dhcp-config)#
In this configuration mode, you can configure the IP address range, the DNS server and the default gateway.

Configuration Examples The following example defines a DHCP address pool with the name mypool0.

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)#
```

Related Commands

Command	Description
host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
ip dhcp excluded-address	Defines the IP addresses that the DHCP server cannot assign to the clients.
network (DHCP)	Defines the network number and network mask of the DHCP address pool.

Platform Description N/A

ip dhcp use class

Use this command to enable the class to allocate addresses in global configuration mode. Use the **no** form of this command to disable the class.
ip dhcp use class
no ip dhcp use class

Parameter Description

Parameter	Description
N/A	N/A

Defaults The class can allocate addresses by default.

Command Mode Global configuration mode

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

lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in DHCP address pool configuration mode. Use the **no** form of this command to restore the default configuration.

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 is 1 day by default.

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 renewing the lease. In general, the DHCP server will allow renewing the lease of the original IP address.

Configuration Examples The following example sets the DHCP lease to 1 hour.

```
Ruijie(dhcp-config)# lease 0 1
```

The following example sets the DHCP lease to 1 minute.

```
Ruijie(dhcp-config)# lease 0 0 1
```

Related

Command	Description

Commands		
	ip dhcp pool	Defines the name of the DHCP address pool and enters DHCP address pool configuration mode.

Platform Description N/A

netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in DHCP address pool configuration mode. Use the **no** form of this command to delete the WINS server.

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 eight 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.

```
Ruijie(dhcp-config)# 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 DHCP address pool configuration mode.

Platform Description N/A

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 delete the configuration of the NetBIOS node type.

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 four 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 to Hybrid.

Configuration Examples The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

```
Ruijie(dhcp-config)# netbios-node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Defines the name of DHCP address pool and enter DHCP address pool configuration mode.
netbios-name-server	Configures the WINS name server of the Microsoft DHCP client NETBIOS.

Platform Description N/A

network (DHCP)

Use this command to define the network number and network mask of the DHCP address pool. Use the **no** form of this command to delete the definition.

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 in priority order. 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 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.

```
Ruijie(dhcp-config)# 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 DHCP address pool configuration mode.

Platform Description N/A

next-server

Use this command to define the startup sever list that the DHCP client accesses during startup. Use the **no** form of this command to delete the definition of the startup server list.

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) Configures IP addresses of up to eight startup servers.

Defaults N/A

Command Mode DHCP address pool configuration mode

Usage Guide When multiple servers are 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.

```
Ruijie(dhcp-config)# next-server 192.168.12.4
```

Related Commands

Command	Description
bootfile	Defines the default startup mapping file name of the DHCP client.
ip dhcp pool	Defines the name of the DHCP address pool and enters 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

option 6rd

Use this command to configure the 6RD parameter. Use the **no** form of this command to restore the default setting.

option 6rd ipv4masklen <*mask-length*> **ipv6prefixlen** <*prefix-length*> **ipv6prefix** <*ipv6-prefix*> **br-addr** <*ipv4-address*>

no option 6rd

Parameter Description

Parameter	Description
mask-length	Generic IPv4 prefix and suffix length, in the range from 0 to 32.
prefix-length	IPv6 prefix length. (32 - *mask-length*) + *prefix-length* <= 128
ipv6-prefix	IPv6 address prefix.
ipv4-address	IPv4 address of the border relay,

Defaults No 6RD parameter is configured by default.

Command Mode DHCP address pool configuration mode

Usage Guide N/A

Configuration Examples The following example specifies the 6RD parameter for the DHCP client.

```
Ruijie(dhcp-config)#option 6rd ipv4masklen 16 ipv6prefixlen 32 ipv6prefix 2002:DA8:: br-addr 1.1.1.1
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client to obtain the IP address.
ip dhcp pool	Sets the DHCP address pool name and enters DHCP address pool configuration mode.

Platform Description N/A

option

Use this command to configure the option of the DHCP server. Use the **no** form of this command to delete the definition of option.

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 hexadecimal string.
ip *ip-address*	Defines an IP address list.

Defaults N/A

Command Mode DHCP address pool 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 at least 312 bytes of option information. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the current definition of DHCP option, see the *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 following configuration enables 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 DHCP address pool configuration mode.

Platform Description N/A

relay agent information

Use this command to enter Option82 matching information configuration mode in 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 Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Global class configuration mode

Mode

Usage Guide After executing this command, the system enters Option82 matching information configuration mode which is shown as “Ruijie (config-dhcp-class-relayinfo)#”.
In this configuration mode, you can configure the class matching multiple pieces of Option82 information.

Configuration Examples The following example configures a global class and enters 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 global class configuration mode.

Platform Description N/A

relay-information hex

Use this command to enter 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 value with the asterisk (‘*) means partial matching which only the front part needs to be matched. The value without the asterisk (‘*) 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 pieces of 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 enters global CLASS configuration mode.
relay agent information	Enters Option82 matching information configuration mode.

Platform Description N/A

remark

Use this command to configure the identification which is used to describe the class in 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 spaces 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 enters global class configuration mode.

Platform N/A

Description

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 disable the DHCP server and the DHCP relay agent.

service dhcp

no service dhcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The DHCP server and the DHCP relay agent are disabled by default.

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 the configuration information about the 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 agent on the device.

```
Ruijie(config)# service dhcp
```

Related Commands

Command	Description
show ip dhcp server statistics	Shows various statistics information of the DHCP server.

Platform Description N/A

clear ip dhcp binding

Use this command to clear the DHCP binding table in privileged EXEC mode.

clear ip dhcp binding { * | *ip-address* }

Parameter Description

Parameter	Description
*	Deletes all DHCP bindings.

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.

Ruijie# **clear ip dhcp binding** *192.168.12.100*

Related Commands

Command	Description
show ip dhcp binding	Shows the address binding of the DHCP server.

Platform Description N/A

clear ip dhcp conflict

Use this command to clear the DHCP address conflict record in privileged EXEC mode.

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.

Ruijie# **clear ip dhcp conflict** *

Related Commands

Command	Description
ip dhcp ping packets	Defines the number of the 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	Shows the address conflict that the DHCP server detects when it assigns an IP address.

Platform Description N/A

clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in privileged EXEC 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 counter of the DHCP server records the entries of the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also collects statistics about the number of sent and received DHCP packets. The **clear ip dhcp server statistics** command can be used to delete the history counter record and restart the statistics collecting.

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	Shows the statistics record of the DHCP server.

Platform Description N/A

debug ip dhcp client

Use this command to debug the DHCP client in privileged EXEC mode.

debug ip dhcp client

no debug ip dhcp client

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide This command shows the main packet content of the DHCP client during its interaction with the servers and the processing status.

Configuration Examples The following example enables the debugging of the DHCP client on the device.

```
Ruijie# debug ip dhcp client
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug ip dhcp server

Use this command to debug the DHCP server in privileged EXEC mode.

debug ip dhcp server { **event** | **packet** }

no debug ip dhcp server { **event** | **packet** }

Parameter Description

Parameter	Description
event	Shows the DHCP message.
packet	Shows the DHCP packet.

Defaults This command is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide This command is used to show the main packet content of the DHCP server during its interaction with the client and the processing status.

Configuration Examples The following example enables the debugging of the DHCP server on the device.

```
Ruijie# debug ip dhcp server packet
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show dhcp lease

Use this command to show the lease information of the IP address obtained by the DHCP client in

privileged EXEC mode.

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, the command shows the binding of all addresses. If the IP address is defined, the command shows the binding of this IP address.

Configuration Examples The following is the command output.

```
Ruijie# show dhcp lease
Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0
Temp sub net mask: 255.255.255.0
 DHCP Lease server: 192.168.5.70, state: 3 Bound
 DHCP transaction id: 168F
 Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
 Next timer fires after: 00:04:29
 Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Fa0/0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show ip dhcp binding

Use this command to show the binding condition of the DHCP address in privileged EXEC mode.

show ip dhcp binding [*ip-address*]

Parameter Description	Parameter	Description
	ip-address	(Optional) Shows 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, the command shows the binding condition of all addresses. If the IP address is defined, the command shows the binding condition of this IP address

Configuration Examples The following is the command output.

```
Ruijie# show ip dhcp binding
IP address Client-Identifier/ Lease expiration Type
      Hardware address
192.168.1.2 00d0.f866.4777    IDLE       Manual
```

The following table describes the fields in the command output.

Field	Description
IP address	IP address to be assigned to the DHCP client
Client-Identifier /Hardware address	Client identifier or hardware address of the DHCP client
Lease expiration	Expiration date of the lease. The Infinite indicates it is not limited by the time. *IDLE* indicates the address is in the free status currently for it is not renewed or the DHCP client releases it initiatively.
Type	Type of the address binding. *Automatic* indicates an IP address is assigned automatically, and *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

show ip dhcp conflict

Use this command to show the conflict record of the DHCP sever in privileged EXEC mode.

show ip dhcp conflict

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command shows the conflict address list and the excluded-address list detected by the DHCP

server.

Configuration Examples

The following is the command output.

```
IP address        Detection Method
192.168.12.1      Ping
dhcp excluded ipaddress
192.168.12.100
```

The following table describes fields in the command output.

Field	Description
IP address	IP addresses which cannot be assigned to the DHCP client.
Detection Method	Conflict detection method.

Related Commands

Command	Description
clear ip dhcp confict	Clears the DHCP conflict record.

Platform Description

N/A

show ip dhcp server statistics

Use this command to show the statistics of the DHCP server in privileged EXEC mode.

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 shows the statistics of the DHCP server.

Configuration Examples

The following is the command output.

```
Ruijie# show ip dhcp server statistics
Lease count       7
Address pools     4
Automatic bindings   4
Manual bindings    0
```

```
Expired bindings     0
Malformed messages 2
Message         Received
BOOTREQUEST       216
DHCPDISCOVER       33
DHCPREQUEST       25
DHCPDECLINE       0
DHCPRELEASE       1
DHCPINFORM       150
Message         Sent
BOOTREPLY         16
DHCPOFFER         9
DHCPACK         7
DHCPNAK         0
```

The following table describes fields in the command output.

Field	Description
Lease count	Number of allocated lease
Address pools	Number of address pools
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	Deletes the DHCP server statistics.

Platform Description N/A

dhcp-server help

Use this command to show the configuration example of the DHCP server.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure and misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples After you enter the **dhcp-server help** command:

```
//配置DNS服务器地址
--------------------------------------------------------------------------------

Ruijie#
```

English interface:

```
Ruijie#dhcp-server help

---------------------------- Configuration Requirements ----------------------------
The client PC is connected to the network of the the DHCP server and
dynamically obatains the configurations from the DHCP server such as IP
address. The IP address of the interface Gi0/2 (connecting with clients) of
DHCP server is 10.10.0.1/16.

------------------------------ Configuration Steps ------------------------------
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 10.10.0.1 255.255.0.0
Ruijie(config-if)#exit
//Configure the IP address of the interface Gi 0/2 that connects with clients

Ruijie(config)#service dhcp
//Enable the DHCP server
Rujie(config)#ip dhcp excluded-address 10.10.0.1 10.10.0.10
//Configure the DHCP excluded addresses which won't be allocated to clients

Ruijie(config)#ip dhcp pool mypool
//Configure the address pool named "mypool" and enter the address pool
configuration mode
Ruijie(dhcp-config)#network 10.10.0.0 255.255.0.0
//Configure the range of DHCP address pool

Ruijie(dhcp-config)#default-router 10.10.0.1
//Configure the default gateway of client
Ruijie(dhcp-config)#dns-server 10.10.0.2
//Configure the address of DNS server
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

dhcp help

Use this command to show the configuration example of the DHCP.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples After you enter the **dhcp help** command:

```
Ruijie(config-if)#ip address 10.10.0.3 255.255.0.0
//配置与客户端设备连接的端口的IP地址
Ruijie(config-if)#view dhcp-relay
//查看DHCP中继信息
--------------------------------------------------------------------------------
```

English interface:

```
Ruijie#dhcp help

--------------------------------- Example Menu ---------------------------------
1. DHCP Server configuration example
2. DHCP Relay configuration example
3. DHCP Snooping configuration example

--------------------------------------------------------------------------------
Please choose the number you want to view (Press the ESC to exit):
```

Enter **1** to view configuration example 1.

```
Ruijie#dhcp help

--------------------------------- Example Menu ----------------------------------
1. DHCP Server configuration example
2. DHCP Relay configuration example
3. DHCP Snooping configuration example

---------------------------------------------------------------------------------
Please choose the number you want to view (Press the ESC to exit): 1

-------------------------- Configuration Requirements ---------------------------
The client PC is connected to the network of DHCP server and obtains dynamically
the configurations from the DHCP server such as IP address. The IP address of
the interface Gi0/2 (connecting with clients) of DHCP server is 10.10.0.1/16.

------------------------------ Configuration Steps ------------------------------
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 10.10.0.1 255.255.0.0
Ruijie(config-if)#exit
//Configure the IP address of the interface Gi 0/2 that connects with clients

Ruijie(config)#service dhcp
//Enable the DHCP server
Ruijie(config)#ip dhcp excluded-address 10.10.0.1 10.10.0.10

//Configure the DHCP excluded addresses which won't be allocated to clients

Ruijie(config)#ip dhcp pool mypool
//Configure the address pool named "mypool" and enter the address pool
  configuration mode
Ruijie(dhcp-config)#network 10.10.0.0  255.255.0.0
//Configure the range of DHCP address pool
Ruijie(dhcp-config)#default-router 10.10.0.1
//Configure the default gateway of client
Ruijie(dhcp-config)#dns-server 10.10.0.2
//Configure the address of DNS server
---------------------------------------------------------------------------------
```

Enter **2** to view configuration example 2.

```
Ruijie#dhcp help

--------------------------------- Example Menu ----------------------------------
1. DHCP Server configuration example
2. DHCP Relay configuration example
3. DHCP Snooping configuration example

---------------------------------------------------------------------------------
Please choose the number you want to view (Press the ESC to exit): 2

-------------------------- Configuration Requirements ---------------------------
The client PCs in the network segment of 10.10.0.0/16 requires to apply for IP
addresses from the DHCP server 2.1.1.1/24 through DHCP relay.

------------------------------ Configuration Steps ------------------------------
1) Configure the DHCP Server
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 2.1.1.1 255.255.255.0
Ruijie(config-if)#exit
//Configure the IP address of the interface Gi 0/2 that connects with DHCP Relay

Ruijie(config)#service dhcp
//Enable the DHCP server
Ruijie(config)#ip dhcp excluded-address 10.10.0.1 10.10.0.10
```

```
//Configure the DHCP excluded addresses which won't be allocated to clients
Ruijie(config)#ip dhcp pool mypool
//Configure the address pool named "mypool" and enter the address pool
  configuration mode
Ruijie(dhcp-config)#network 10.10.0.0  255.255.0.0
//Configure the range of DHCP address pool
Ruijie(dhcp-config)#default-router 10.10.0.1
//Configure the default gateway of client
Ruijie(dhcp-config)#dns-server 10.10.0.2
//Configure the address of DNS server
Ruijie(dhcp-config)#view dhcp-server
//View the DHCP server information

2) Configure the DHCP Relay
Ruijie(config)#server dhcp
//Enable the DHCP relay agent
Ruijie(config)#ip helper-address 2.1.1.1
//Add a global DHCP server address
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 2.1.1.2 255.255.255.0
//Configure the IP address for the port connecting with Server device

Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 10.10.0.3 255.255.0.0
//Configure the IP address for the port connecting with client device
Ruijie(config-if)#view dhcp-relay
//View the DHCP relay information
--------------------------------------------------------------------------------
```

Enter **3** to view configuration example 3.

```
Ruijie#dhcp help

---------------------------------- Example Menu ----------------------------------
1. DHCP Server configuration example
2. DHCP Relay configuration example
3. DHCP Snooping configuration example

--------------------------------------------------------------------------------
Please choose the number you want to view (Press the ESC to exit): 3

--------------------------- Configuration Requirements ---------------------------
Enable the DHCP Snooping on the access device, so as to avoid illegal users from
setting private DHCP servers.

------------------------------ Configuration Steps -------------------------------
Ruijie#configure terminal
Ruijie(config)#ip dhcp snooping
//Enable the DHCP Snooping

Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#ip dhcp snooping trust
//Configure the interface connecting with DHCP server as a TRUST port. Only the
DHCP reply packets sent from the server connected to a TRUST port can be
forwarded. By default, all ports are UNTRUST ports.
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp excluded-address help

Use this command to show the configuration help of the command that configures the excluded addresses.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp excluded-address help

Examples:
------------------------------------------------------------------------------
>ip dhcp excluded-address 192.168.12.100 192.168.12.150

Define addresses in the range of 192.168.12.100-192.168.12.150 as excluded
addresses, so that the DHCP server won't allocate these addresses to the DHCP
clients.
192.168.12.100:start address;        192.168.12.150:end address;
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp ping help

Use this command to show the configuration help of the command that configures the ping packet.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp ping help

Examples:
--------------------------------------------------------------------------------
>ip dhcp ping packets 3

Specify the number of ping packets sent from the DHCP server in order to verify
whether the address to be allocated has been used by any other host to 3
(default: 2). The number of ping packets sent ranges from 0 to 10, and 0 means
to disable the ping.
--------------------------------------------------------------------------------
>ip dhcp ping timeout 600

Specify the amount of time that the DHCP server waits for a ping reply after
sending ping packets to verify whether the address to be allocated has been
used by any other host to 600ms (default: 500ms). The amount of time that the
DHCP server waits for ping reply ranges from 100 to 10000 (in milliseconds).
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp pool help

Use this command to show the configuration help of the command that configures the address pool.

Parameter

Parameter	Description

Description

N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp pool help

Examples:
------------------------------------------------------------------------------
>ip dhcp pool mypool

Create a dhcp address pool "mypool" and enter the address pool configuration
mode.
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

bootfile help

Use this command to show the configuration help of default startup image file required by the DHCP client.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#bootfile help

Examples:
------------------------------------------------------------------------------
>bootfile router.conf

Provide the image file of "router.conf" required by certain DHCP clients at
start-up, so that the client can download the image file via the corresponding
server (such as TFTP).
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

default-router help

Use this command to show the help information about defining the default gateway of the DHCP client.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?).

However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples

English interface:

```
Ruijie(dhcp-config)#default-router help

Examples:
------------------------------------------------------------------------------
>default-router 192.168.12.1

Specify 192.168.12.1 as the default gateway of clients. This address must be in
the same network segment as the addresses allocated to clients. There must be
at least one default gateway, and up to 8 gateways can be configured.
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

lsase help

Use this command to show the help information about defining the lease time of the address assigned to the client by the DHCP server.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#lease help

Examples:
------------------------------------------------------------------------------
>lease 0 1 2

Set the DHCP lease period as 1 hour and 2 minutes.
0: day (default: 1);                  1: hour (default: 0);
2: minute (default: 0);
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

domain-name help

Use this command to show the help information about defining the suffix domain name of the DHCP client.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode N/A

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#domain-name help

Examples:
------------------------------------------------------------------------------
>domain-name i-net.com.cn

Specify the suffix domain name "i-net.com.cn" for DHCP clients.
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

dns-server help

Use this command to show the help information about defining the DNS server of the DHCP client.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#dns-server help

Examples:
------------------------------------------------------------------------------
>dns-server 192.168.12.3

Specify the DNS server "192.168.12.3" for DHCP clients. There must be at least
one DNS server, up to 8 DNS servers can be configured.
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

netbios-name-server help

Use this command to show the help information about configuring the WIS name server of the DHCP client NETBIOS.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#netbios-name-server help

Examples:
------------------------------------------------------------------------------
>netbios-name-server 192.168.12.3

Specify the WINS server "192.168.12.3" for DHCP clients. You can configure up
to 8 WINS servers.
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

netbios-node-type help

Use this command to show the help information about defining the NetBIOS node type of the Microsoft DHCP client.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#netbios-node-type help

Examples:
--------------------------------------------------------------------------------
>netbios-bios-type h-node

Set the NetBIOS node of the Microsoft DHCP client as a hybrid node.
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

network help

Use this command to show the help information about defining the network number and network

mask of the DHCP address pool.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#network help

Examples:
--------------------------------------------------------------------------------
>network 192.168.12.0 255.255.255.240

Specify the network number of DHCP address pool as 192.168.12.0, with mask
255.255.255.240, so as to provide the DHCP server with an address space
allocable to clients.
192.168.12.0: IP network number of address pool;
255.255.255.240: IP network mask of address pool;
--------------------------------------------------------------------------------
```

You can use the language {chinese | english} command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

host help

Use this command to show the help information about defining the statically bound IP address and network mask of the DHCP address pool.

Parameter

Parameter	Description

Description

N/A	N/A

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#host help

Examples:
------------------------------------------------------------------------------
>host 192.168.12.91 255.255.255.240

Specify the IP address and network mask of the DHCP client in the address pool,
so as realize the static mapping between the client IP and MAC address in the
DHCP server database.
192.168.12.91: Client IP address;
255.255.255.240: Network mask of client host;
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

relay help

Use this command to show the help information about class configuration mode.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Class configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples

English interface:

```
Ruijie(config-dhcp-class)#relay help

Examples:
--------------------------------------------------------------------------------
>relay agent information

Enter the Option 82 matching information configuration mode.
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

relay-information help

Use this command to show the help information about class configuration mode.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Option82 matching information configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can

improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples

English interface:

```
Ruijie(config-dhcp-class-relayinfo)#relay-information help

Examples:
------------------------------------------------------------------------------
>relay-information hex 010225654565

Configure the specific Option 82 matching information; The 010225654565 is
hexadecimal Option82 matching information.
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

remark help

Use this command to show the help information about class configuration mode.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Class configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp use help

Use this command to show the help information about enabling the DHCP service.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp use help

Examples:
--------------------------------------------------------------------------------
>ip dhcp use class

Enable the address allocation using CLASS.
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp database help

Use this command to show the help information about saving the configured DHCP binding database.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp database help

Examples:
--------------------------------------------------------------------------------
>ip dhcp database help

Configure the delay time for writing the DHCP Snooping database into FLASH as
3600 seconds (default: 0), as to as avoid the loss of binding database (lease
information) on DHCP server when the device restarts due to an electricity
failure.
--------------------------------------------------------------------------------
>ip dhcp database write-to-flash

Manually write the binding database into the FLASH, so as to avoid the loss of
DHCP binding database (lease information) when the device restarts due to an
electricity failure.
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

class help

Use this command to show the help information about enabling the address assignment using the class.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(dhcp-config)#class help

Examples:
--------------------------------------------------------------------------------
>class class1

Configure the name of CLASS associated with the address pool as "class1" and
enter the CLASS configuration mode of the address pool.
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

address help

Use this command to show the information about configuring the class network segment associated with the address pool.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Class configuration mode of the address pool

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config-dhcp-pool-class)#address help

Examples:
------------------------------------------------------------------------------
>address range 172.16.1.1 172.16.1.8

Configure the address range of class1 associated with the address pool to
"172.16.1.1-172.16.1.8".
172.16.1.1: start address of address range;
172.16.1.8: end address of address range;
------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.

In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp help

Examples:
--------------------------------------------------------------------------------
>ip dhcp excluded-address 192.168.12.100 192.168.12.150

Define addresses in the range of 192.168.12.100-192.168.12.150 as excluded
addresses, so that the DHCP server won't allocate these addresses to the DHCP
clients.
192.168.12.10: start address;                192.168.12.150: end address;
--------------------------------------------------------------------------------
>ip dhcp pool mypool

Create the dhcp address pool "mypool" and enter the address pool configuration
mode
--------------------------------------------------------------------------------
>ip dhcp relay information option82

Enable the DHCP relay option82 function. The server can allocate different IP
addresses to users according to the option82 information. This function will
conflict with the option dot1x. They can not be configured at the same time.
--------------------------------------------------------------------------------
>ip dhcp snooping vlan 1000

Enable the DHCP Snooping on the VLAN1000. This function will take effect only
after DHCP Snooping has been enabled globally.
--------------------------------------------------------------------------------
>ip dhcp class myclass

Define a CLASS (name: myclass) and enter the global CLASS configuration mode.
The specific Option82 matching information corresponding to each CLASS can be
configured after entering the global CLASS configuration mode.
--------------------------------------------------------------------------------
```

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

view dhcp-server

Use this command to show the information about the DHCP server module.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode This command can be executed in any modes.

Usage Guide Currently, you can use two commands on the CLI to respectively show the configurations. For the required information of a specific state, you must use several related commands, which is complex. For simplification, it is necessary to show the status information together with the related configurations.

Configuration Examples

```
Ruijie#view dhcp-server

Address pools: 4
                          Total        Distributed   Remaining
Pool name   Class         addreses     addresses     addresses   Address range
----------  ----------    ----------   ----------    ----------  -----------------
mypool1     myclass1      100          100           100         192.168.200.1-
                                                                 192.168.200.100
mypool1     myclass2      100          20            80          192.168.200.101-
                                                                 192.168.200.200
mypool2     hello         200          200           0           172.16.56.1-
                                                                 172.16.56.200
……
More information, refer to: show dhcp-server pool

Ip conflict times:10
Ip address         Dedection method
-----------------  -----------------
10.77.21.90        Ping
10.77.21.92        Ping
10.77.25.132       Ping
……
More information, refer to: show ip dhcp conflict
```

```
Automatic bindings:    4
Manual bindings:       0
Expired bindings:      0
Malformed messages:    2
More information, refer to: show ip dhcp binding

Message             Received
--------------      -------------
BOOTREQUEST         216
DHCPDISCOVER        33
DHCPREQUEST         25
DHCPDECLINE         0
DHCPRELEASE         1
DHCPINFORM          150

Message             Sent
--------------      ------------
BOOTREPLY           16
DHCPOFFER           9
DHCPACK             7
DHCPNAK             0

Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show dhcp-server pool

Use this command to show the information about the address pool.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode This command can be executed in any modes.

Usage Guide Currently, you can use two commands on the CLI to respectively show the configurations and the status information. For the required information of a specific state, you must use several related commands, which is complex. For simplification, it is necessary to show the status information together with the related configurations.

Configuration Examples

```
Ruijie#show dhcp-server pool

                          Total        Distributed   Remaining
Pool name   Class         addreses     addresses     addresses   Address range
----------  ----------    -----------  ------------  ----------  -----------------
mypool1     myclass1      100          100           100         192.168.200.1-
                                                                 192.168.200.100
mypool1     myclass2      100          20            80          192.168.200.101-
                                                                 192.168.200.200
mypool2     hello         200          200           0           172.16.56.1-
                                                                 172.16.56.200
mypool2     world         50           45            5           172.16.56.201-
                                                                 172.16.56.250
mypool3     ---           150          145           5           192.168.217.1-
                                                                 192.168.217.150
mypool4     xukai         110          110           0           10.1.1.1-
                                                                 10.1.1.110
mypool4     linhaimei     40           30            10          10.1.1.111-
                                                                 10.1.1.150
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

view dhcp

Use this command to show the information about the DHCP configuration and status.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode This command can be executed in any modes.

Usage Guide Currently, you can use two commands on the CLI to respectively show the configurations and the status information. For the required information of a specific state, you must use several related commands, which is complex. For simplification, it is necessary to show the status information together with the related configurations.

Configuration Examples

```
Ruijie#view dhcp

Dhcp server:   enabled
Dhcp relay:    enabled
Dhcp snooping: enabled

Dhcp server information
********************************************************************************
Address pools: 4
                          Total         Distributed   Remaining
Pool name   Class         addreses      addresses     addresses   Address range
----------  ----------    ----------    ----------    ----------  -----------------
mypool1     myclass1      100           100           100         192.168.200.1-
                                                                  192.168.200.100
mypool1     myclass2      100           20            80          192.168.200.101-
                                                                  192.168.200.200
mypool2     hello         200           200           0           172.16.56.1-
                                                                  172.16.56.200
……
More information, refer to: show dhcp-server pool

Ip conflict times:10
Ip address         Dedection method
-----------------  -----------------

10.77.21.90        Ping
10.77.21.92        Ping
10.77.25.132       Ping
……
More information, refer to: show ip dhcp conflict

Automatic bindings:    4
Manual bindings:       0
Expired bindings:      0
Malformed messages:    2
More information, refer to: show ip dhcp binding

Message              Received
---------------      -------------
BOOTREQUEST          216
DHCPDISCOVER         33
DHCPREQUEST          25
DHCPDECLINE          0
--Press Space or Enter to continue, press any key to exit--
DHCPRELEASE          1
DHCPINFORM           150

Message              Sent
---------------      -------------


BOOTREPLY            16
DHCPOFFER            9
DHCPACK              7
DHCPNAK              0

Dhcp relay information
********************************************************************************
dhcp client net       dhcp relay information     dhcp server          user number
-------------------   -----------------------    ------------------   -------------
10.10.1.1/16          option dot1x               30.0.0.2             20
20.20.1.1/16          option dot1x               30.0.0.2             10
20.21.1.1/16          option dot1x               30.0.0.2             20
……
More information, refer to: show ip dhcp relay user

Dhcp snooping information
********************************************************************************
Total number of bindings: 10
MacAddress          IpAddress        Lease(sec)   Type           VLAN  Interface
------------------- ---------------- ------------ -------------- ----- ------------
0000.0000.0001      192.168.12.1     78128        dhcp-snooping  1     Gi 0/1
00d0.f800.0001      192.168.10.1     50000        dhcp-snooping  2     Gi 0/2
00d0.f822.0002      192.168.11.1     78000        dhcp-snooping  10    Gi 0/6
……
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

DHCP Relay Commands

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 disable the **ip dhcp relay check** *server-id* function.

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* function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to select the destination DHCP server according to server-id option when forwarding a DHCP request. If this comand is not configured, the DHCP request is forwarded to all 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

ip dhcp relay information option dot1x

Use this command to enable the **dhcp option dot1x** function of DHCP relay.

Use the **no** form of the command to disable the **dhcp option dot1x** function.

ip dhcp relay information option dot1x

no ip dhcp relay information option dot1x

Parameter

Parameter	Description

Description

N/A	N/A

Defaults The **dhcp option dot1x** function is disabled by default.

Command Mode Global configuration mode

Usage Guide It is necessary to enable the DHCP Relay, and combine with the 802.1x related configuration to configure this command.

Configuration Examples The following example enables the DHCP option dot1x function on the device.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay information option dot1x
```

Related Commands

Command	Description
service dhcp	Enables the DHCP Relay.
ip dhcp relay information option dot1x access-group	Configures the option dot1x acl.

Platform Description N/A

ip dhcp relay information option dot1x access-group

Use this command to configure the ACL associated with the **DHCP relay option dot1x**. Use the **no** form of this command to disable the ACL associated with the **DHCP relay option dot1x**.

ip dhcp relay information option dot1x access-group *acl-name*

no ip dhcp relay information option dot1x access-group *acl-name*

Parameter Description

Parameter	Description
N/A	N/A

Defaults No ACL is associated by default.

Command Mode Global configuration mode

Usage Guide Ensure that the ACL does not conflict with the existing ACE of the configured ACL on the interface.

Configuration Examples The following example enables the dhcp option dot1x acl function.

```
Ruijie# configure terminal
```

```
Ruijie(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
Ruijie(config-ext-nacl)# permit ip any host 192.168.3.1
//Permit sending the packets to the gateway.
Ruijie(config-ext-nacl)# permit ip any host 192.168.4.1
Ruijie(config-ext-nacl)# permit ip any host 192.168.5.1
Ruijie(config-ext-nacl)# permit ip host 192.168.3.1 any
// Permit the communication between the packets whose source IP address is that of the gateway.
Ruijie(config-ext-nacl)# permit ip host 192.168.4.1 any
Ruijie(config-ext-nacl)# permit ip host 192.168.5.1 any
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
//Deny the exchange between the unauthenticated users.
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.5.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255
Ruijie(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255
Ruijie(config-ext-nacl)# exit
Ruijie(config)# ip dhcp relay information option dot1x access-group
DenyAccessEachOtherOfUnauthrize
```

Related Commands

Command	Description
service dhcp	Enables DHCP relay.
ip dhcp relay information option dot1x	Enable the DHCP option dot1x function.

Platform Description N/A

ip dhcp relay information option82

Use this command to configure to enable the **option82** function of DHCP relay. Use the **no** form of this command to disable the function.

ip dhcp relay information option82

no ip dhcp relay information option82

Parameter Description

Parameter	Description
N/A	N/A

Defaults The option82 function of DHCP relay is disabled by default.

Command Mode Global configuration mode

Usage Guide This function is exclusive with the option dot1x function.

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.
ip dhcp relay information option dot1x	Enables the DHCP option dot1x function.

Platform Description N/A

ip dhcp relay suppression

Use this command to enable the DHCP relay suppression function on a specified interface. Use the **no** form of this command to disable ththis function.

ip dhcp relay suppression

no ip dhcp relay suppression

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is disabled by default.

Command Mode Interface configuration mode

Usage Guide After this command is executed, the system will not relay the DHCP request message on the interface.

Configuration Examples The following example enables the DHCP relay suppression function on 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

Command	Description

Commands		
	service dhcp	Enables the DHCP relay.

Platform Description N/A

ip helper-address

Use this command to add the IP address of a DHCP server. Use the **no** form of this command to delete the IP address of the DHCP server.

The server address can be configured in global configuration mode or interface configuration mode.

ip helper-address [**vrf** *vrf-name*]*A.B.C.*

no ip helper-address [**vrf** *vrf-name*]*A.B.C.*

Parameter Description	Parameter	Description
	N/A	N/A

Defaults No server address is configured by default.

Command Mode Global configuration mode, or interface configuration mode

Usage Guide Up to 20 DHCP server can be configured globally or on each layer-3 interface.

If the DHCP server address is not configured on the interface, the DHCP relay uses the address of the global DHCP server. If the DHCP address is configured on the interface, the DHCP relay uses the configured server address.

For the *vrf* parameter, the global configuration and interface-based configuration are slightly different. In global configuration mode, if the vrf parameter is not specified, the default address of the current server does not belong to any vrf. In interface-based configuration, if the *vrf* parameter is not specified, the current default server and port configurations belong to the same vrf.

Configuration Examples The following example:

1. Configures the IP address for the global server to 192.168.1.1.
2. Configures 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 N/A

Description

service dhcp

Use this command to enable the DHCP relay in global configuration mode. Use the **no** form of this command to disable this function.

no service dhcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The DHCP relay can forward the DHCP request to other servers and the DHCP response packets to the DHCP client, serving as the relay for DHCP packets.

Configuration Examples The following configuration example enables the DHCP relay.

```
Ruijie# configure terminal
Ruijie(config)# service dhcp
```

Related Commands

Command	Description
ip helper-address	Adds the IP address of an DHCP server.

Platform Description N/A

dhcp-relay help

Use this command to show the help information about configuring the DHCP relay.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the next keyword or parameter with related description will be displayed after the question mark (?). However, the description may be obscure misleading.

In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples After you enter the dhcp-relay help command:

English interface:

```
Ruijie#dhcp-relay help

------------------------------ Configuration Requirements ------------------------
The client PCs in the network segment of 10.10.0.0/16 need to apply for the IP
addresses from DHCP server 2.1.1.1/24 through DHCP relay.

--------------------------------- Configuration Steps ---------------------------
1) Configure the DHCP Server
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 2.1.1.1 255.255.255.0
Ruijie(config-if)#exit
//Configure the IP address of the interface Gi 0/2 that connects with the DHCP
  Relay

Ruijie(config)#service dhcp
//Enable the DHCP server
Ruijie(config)#ip dhcp excluded-address 10.10.0.1 10.10.0.10
//Configure the DHCP excluded addresses which won't be allocated to clients
Ruijie(config)#ip dhcp pool mypool
//Configure the address pool named "mypool" and enter the address pool
  configuration mode
Ruijie(dhcp-config)#network 10.10.0.0 255.255.0.0
//Configure the range of the DHCP address pool
Ruijie(dhcp-config)#default-router 10.10.0.1

//Configure the default gateway of the client
Ruijie(dhcp-config)#dns-server 10.10.0.2
//Configure the DNS server address
Ruijie(dhcp-config)#view dhcp-server
//View the DHCP server information

2) Configure the DHCP Relay
Ruijie(config)#service dhcp
//Enable the DHCP relay agent
Ruijie(config)#ip helper-address 2.1.1.1
//Add a global DHCP server address
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 2.1.1.2 255.255.255.0
//Configure the IP address for the port connecting with Server device

Ruijie(config)#interface gigabitEthernet 0/3
Ruijie(config-if)#no switchport
Ruijie(config-if)#ip address 10.10.0.3 255.255.0.0
//Configure the IP address for the port connecting with client device
Ruijie(config-if)#view dhcp-relay
//View the DHCP relay information
--------------------------------------------------------------------------------
```

Note You can use the language {chinese | english} command in privileged mode to switch interfaces.

Related Commands

Command	Description
view dhcp-relay	Shows the information about the DHCP server module.

Platform Description N/A

ip dhcp relay help

Use this command to show the help information about configuring the DHCP relay.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode or interface configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the next keyword or parameter with related description will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples Global configuration mode

English interface:

```
Ruijie(config)#ip dhcp relay help

Examples:
--------------------------------------------------------------------------------
>ip dhcp relajy check server-id

Enable the check server-id function of the DHCP relay. After configuring this
function, the DHCP relay will only forward the DHCP request packets to the
server specified in the option server-id.
--------------------------------------------------------------------------------
>ip dhcp relay information option dot1x access-group myacl

Only allow the unauthenticated or low-privilege IPs to access certain IP
addresses, and restrict the mutual access between low-privilege users.
The "myacl" is the preconfigured ACL, and is mainly used to prohibit the
mutual access between unauthenticated users.
--------------------------------------------------------------------------------
>ip dhcp relay information option82

Enable the DHCP relay option82 function. The server can allocate different IP
addresses to users according to the option82 information. This function will
conflict with the option dot1x. They can not be configured at the same time.
--------------------------------------------------------------------------------
>ip dhcp relay information option vpn


Enable the DHCP Relay Aware VRF on the DHCP relay agent. The DHCP relay
deployment requirements under VRF environment can be met by adding the "option".
--------------------------------------------------------------------------------
```

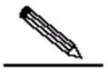
Interface configuration mode

English interface:

```
Ruijie(config-if)#ip dhcp relay help

Examples:
--------------------------------------------------------------------------------
>ip dhcp relay suppression

Enable the DHCP Relay suppression on the specified port. After configuring this
command, the DHCP request packets received on this port will be shielded.
--------------------------------------------------------------------------------
```



Note You can use the language {chinese | english} command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp relay check help

Use this command to show the help information about configuring the check server-id function of the DHCP relay.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the next keyword or parameter with related description will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp relay check help

Examples:
--------------------------------------------------------------------------------
>ip dhcp relay check server-id

Enable the check server-id function of the DHCP relay. After configuring this
function, the DHCP Relay will only forward the DHCP request packets to the
server specified in the option server-id.
--------------------------------------------------------------------------------
```


Note

You can use the language {chinese | english} command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip dhcp relay information help

Use this command to show the help information about adding an option.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the next keyword or parameter with related description will be displayed after the question mark (?). However, the description may be obscure misleading.

In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples English interface:

```
Ruijie(config)#ip dhcp relay information help

Examples:
------------------------------------------------------------------------------
>ip dhcp relay information option dot1x access-group myacl

Only allow the unauthenticated or low-privilege IPs to access certain IP
addresses, and restrict the mutual access between low-privilege users.
The "myacl" is the preconfigured ACL which can be used to filter certain
contents, and is mainly used to prohibit the mutual access between
unauthenticated users.
------------------------------------------------------------------------------
>ip dhcp relay information option82

Enable the DHCP relay option82 function. The server can allocate different IP
addresses to users according to the option82 information. This function will
conflict with the option dot1x. They can not be configured at the same time.
------------------------------------------------------------------------------
>ip dhcp relay information option vpn

Enable the DHCP Relay Aware VRF on the DHCP relay agent. The DHCP relay
deployment requirements under VRF environment can be met by adding the "option".
------------------------------------------------------------------------------
```


Note

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

view dhcp-relay

Use this command to show the information about the DHCP relay module.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode This command can be executed in any modes.

Usage Guide Currently, you can use two commands on the CLI to respectively show the configurations and the status information. For the required information of a specific state, you must use several related commands, which is complex. For simplification, it is necessary to show the status information together with the related configurations.

Configuration Examples

```
Ruijie#view dhcp-relay

dhcp client net      dhcp relay information    dhcp server          user number
-----------------    ----------------------    ------------------   -------------
10.10.1.1/16         option dot1x              30.0.0.2             20
20.20.1.1/16         option dot1x              30.0.0.2             10
20.21.1.1/16         option dot1x              30.0.0.2             20
......
More information, refer to: show ip dhcp relay user

Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

NTP Commands

no ntp

Use this command to disable the **ntp** synchronization service with the time server and clear all configuration information of **ntp**.

no ntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The NTP service is disabled by default.

Command Mode Global configuration mode

Usage Guide By default, the NTP service is disabled. However, the NTP service will be enabled once the NTP server or the NTP security identification mechanism is configured.

Configuration Examples The following example disables the NTP service.

```
Ruijie(config)# no ntp
```

Related Commands

Command	Description
ntp server	Specifies the NTP server.

Platform Description N/A

ntp access-group

Use this command to configure the access control priority of the NTP service. Use the no form of this command to cancel the access control priority.

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 time request for, control and query for the local NTP

	service, as well as time synchronization between the local device and the peer device (full access permission).
serve	Allows the time request for, and control and query for the local NTP service, but not time synchronization between the local device and the peer device
serve-only	Allows the time request for the time of local NTP service.
query-only	Allows the control and query for the local NTP service.
access-list-number	Number of the IP access control list (ACL), in the range 1 to 99 and 1300 to 1999.
access-list-name	Name of the IP ACL

Defaults No NTP access control rule is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the access control priority of the NTP service. The NTP services access control function provides a minimal security measure (the more secure way is to use the NTP authentication mechanism).

When an access request arrives, the NTP service matches the rules in accordance from the smallest to the largest to access restriction, and the first matched rule shall prevail. The matching order is *peer*, *serve*, *serve-only*, and *query-only*.


Caution

The control and query function is not supported in the current system. Although it matches with the order in accordance with the preceding rules, requests related to the control and query function are not supported.


Note

If you do not configure any access control rules, all accesses are allowed. Once the access control rules are configured, only the rule that allows access can be carried out.

Configuration Examples The following example shows how to allow the peer device in acl1 to control, query, request for, and synchronize the time with the local device; and limit the peer device in acl2 to request the time for the local device:

```
Ruijie(config)# ntp access-group peer 1
Ruijie(config)# ntp access-group serve-only 2
```

Related Commands

Command	Description
ip access-list	Creates the IP access control list.

Platform Description N/A

ntp authenticate

Use this command to enable NTP authentication globally.

ntp authenticate

no ntp authenticate

Parameter Description

Parameter	Description
N/A	N/A

Defaults Global NTP authentication is disabled by default.

Command Mode Global configuration mode

Usage Guide If the global security identification mechanism is not used, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the security identification mechanism and configure other keys globally.

The authentication standard is that the trusted key has been specified by **ntp authentication-key** and **ntp trusted-key**.

Configuration Examples The following example enables the authentication mechanism after an authentication key is configured and specified as the global trusted key.

```
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

ntp authentication-key

Use this command to configure a global NTP authentication key for the NTP service.

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

no ntp authentication-key *key-id*

Parameter Description

Parameter	Description
key-id	Key ID
key-string	Key string
enc-type	(Optional) Whether this key is encrypted. **0** indicates the key is not encrypted, and **7** indicates the key is encrypted simply.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Configure the global authentication key and adopt **md5** for encryption. Each key has unique *key-id*. You can use the **ntp trusted-key** to set the key of *key-id as* the global trusted key.
At most 1024 keys are allowed. However, each server can support only one key.

Configuration Examples The following example configures an authentication key with ID 6.

Ruijie(config)# **ntp authentication-key** *6* **md5** *wooooop*

Related Commands

Command	Description
ntp authenticate	Enables the global security identification mechanism.
ntp trusted-key	Configures the global trusted key.
ntp server	Specifies an NTP server.

Platform Description N/A

ntp disable

Use this command to disable the function of receiving the NTP packet on the interface.

ntp disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The NTP packet is received on the interface by default.

Command Interface configuration mode

Mode

Usage Guide The NTP packet received on any interface can be provided to the client to perform the clock adjustment by default. The function can shield the NTP packet received from the corresponding interface.
Note: This command takes effect only for the interface whose IP address can be configured to receive and send packets.

Configuration Examples The following example disables the function of receiving the NTP packet on the interface.

```
Ruijie(config)# no ntp disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ntp master

Use this command to set the local clock as the NTP master (the local clock reference source is reliable), providing the synchronizing time for other devices. Use the **no** form of this command to cancel the NTP master setting.
ntp master [*stratum*]
no ntp master

Parameter Description

Parameter	Description
stratum	Specifies the stratum where of the local clock in the range 1 to 15. The defaut value **8** is used if this parameter is not specified.

Defaults No NTP master is configured by default.

Command Mode Global configuration mode

Usage Guide Generally, the local system synchronizes the time from the external clock source directly or indirectly. However, if time synchronization of local system fails for the network connection trouble, ect, use the command to set the reliable reference source of the local clock, providing the synchronized time for other devices.
Once set, the system time can not be synchronized to the clock source with higher stratum.


Caution Be careful when using this command. Using this command to set the local clock as the

master (in particular, specify a lower stratum value), is likely to cover the effective clock source. If multiple devices in the same network use this command, time synchronization instability may occur due to time difference between the devices.

In addition, before using this command, if the system has never been synchronized with an external clock source, it is necessary to manually calibrate the system clock to prevent too much offset.

Configuration Examples The following example configures the local clock as the NTP master and set the stratum to 12.

```
Ruijie(config)# ntp master 12
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is unavailable on some devices that do not support this function.

ntp server

Use this command to specify an NTP server for the NTP client.

ntp server *ip-addr* [**version** *version*] [**source** *if-name*] [**key** *keyid*] [**prefer**]

no ntp server *ip-addr*

Parameter Description

Parameter	Description
ip-addr	Sets the IP address of the NTP server. IPv4 and IPv6 are supported.
version	(Optional) Specifies the version (1-3) of NTP. The default version is NTPv3.
if-name	(Optional) Specifies the source interface from which the NTP packet is sent (Layer 3 interface).
keyid	(Optional) Specifies the encryption key adopted in communication with the corresponding server.
prefer	(Optional) Specifies the corresponding server as the **Prefer** server.

Defaults No NTP server is configured by default.

Command Mode Global configuration mode

Usage Guide Currently, Ruijie system only acts as clients that can synchronize time from a maximum of 20 servers. To initiate 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. To complete the encrypted communication with the server, the server should have the identical global encryption key and global trust key.
In the same condition (for instance, precision), the prefer clock is used for synchronization.
Note that the NTP-packet-sending source interface is configured with the IP address and can communicate with the corresponding NTP server.

Configuration Examples The following example configures the network device as the NTP server.

IPv4 configuration: Ruijie(config)# **ntp server** *192.168.210.222*
IPv6 configuration: Ruijie(config)# **ntp server** *10::2*

Related Commands

Command	Description
no ntp	Disables the NTP service.

Platform Description This command is unavailable on some devices that do not support this function.

ntp synchronize

Use this command to perform real-time synchronization.
ntp synchronize
no ntp synchronize

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Eight consecutive packets are synchronized for the first synchronization between the client and the server. Follow-up NTP synchronization occurs automatically every one minute. To manually implement real-time synchronization during the auto-synchronization interval, you can use this command.

Configuration Examples The following example implement NTP real-time synchronization.

Ruijie(config)# ntp synchronize

Related Commands

Command	Description
ntp server	Specifies an NTP server and implements

	synchronization.

Platform Description This command is supported only by specific products.

ntp trusted-key

Use this command to set a key corresponding to an ID as 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

Defaults No trusted key is configured by default.

Command Mode Global configuration mode

Usage Guide The NTP communication parties must use the same trusted key. To improve security, the key is identified by ID and is not transmitted.

Configuration Examples The following example configures an authentication key and sets it as the trusted key of corresponding server.

```
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 the security authentication mechanism.
ntp authentication-key	Sets the NTP authentication key.
ntp server	Specifies an NTP server.

Platform Description N/A

ntp update-calendar

Use this command to update the calendar for the NTP client using the time synchronized from an external clock source. Use the **no** form of this command to disable the update-calendar function

ntp update-calendar
no ntp update-calendar

Parameter Description

Parameter	Description
N/A	N/A

Defaults The NTP update-calendar function is not configured by default.

Command Mode Global configuration mode

Usage Guide This function enables NTP clients to update the calendars of devices periodically using the time synchronized from an external clock source. The calendar of the device is still available even if the device is shut down or reset.
By default, the NTP update-calendar function is not configured. After configuration, the NTP client updates the calendar every time the time synchronization of external clock source is successful.

Configuration Examples The following example configures the NTP update-calendar function.

```
Ruijie(config)# ntp update-calendar
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug ntp

Use this command to show NTP debugging information.
debug ntp
no debug ntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to debug the NTP service, export necessary debugging information for failure

diagnosis and troubleshooting.

Configuration Examples The following example enables NTP debugging.

```
Ruijie(config)# debug ntp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ntp status

Use this command to show the NTP information.

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide If the NTP service of the system is enabled, the command shows existing NTP information. This command will display no information until the synchronization server is added for the first time.

Configuration Examples The following example shows the existing NTP information of the system.

```
Ruijie# show ntp status
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ntp help

Use this command to show typical configuration of NTP modules.

ntp help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide For the current operation of the CLI, commands are executed one by one. CLI presentation lacks typical replicable configuration examples for the configuration and deployment of a specific functional module. Therefore, you can only obtain the configuration help by other means (such as reading related manuals and consulting frontline engineers)
In this case, showing typical configurations on the CLI provides the help information about the quick basic deployment of a certain function for users, increasing CLI usability.

Configuration Examples The following is the command output:
The following information is displayed if the example number the user entered is 2:

English interface:

```
Ruijie#ntp help

---------------------------------- Example Menu ----------------------------------
1. NTP client/server mode configuration example
2. NTP client/server ID authentication mode configuration example

--------------------------------------------------------------------------------
Please choose the number you want to view (Press the ESC to exit):
```

The following information is displayed if the example number the user entered is 1:

```
Ruijie#ntp help

---------------------------------- Example Menu ----------------------------------
1. NTP client/server mode configuration example
2. NTP client/server ID authentication mode configuration example

--------------------------------------------------------------------------------
Please choose the number you want to view (Press the ESC to exit):1

--------------------------- Configuration Requirements ---------------------------
Synchronize the clock of newly-purchased deviceB based on deviceA and set the
synchronized time to the hardware of deviceB. Set the deviceA IP address 1.1.1.1
and clock layer 12.

------------------------------ Configuration Steps -------------------------------
1. NTP server configuration
DeviceA(config)#interface vlan 1
DeviceA(config-vlan 1)#ip address 1.1.1.1 255.255.255.0
DeviceA(config-vlan 1)#exit
//Configure the IP address of server.
DeviceA(config)#ntp master 12
//Set the local clock as reference clock(clock layer 12) and enable the ntp
server function. The number of clock layer determines the clock accuracy, in the
range of 1-15 (default:8). Smaller layer means the higher accuracy.
DeviceA(config)#show clock
```

```
    //View current time of the server.

    2. NTP client configuration
    DeviceB(config)#show clock
    //View the device B time before synchronization.
    DeviceB(config)#ntp server 1.1.1.1
    //Designate the deviceA as clock source of deviceB (namely server), enable the
    ntp client function.
    DeviceB(config)#view ntp
    //View whether the synchronization is successful.

    DeviceB(config)#ntp update-calendar
    //Enable NTP hardware clock update to synchronize the hardware time.
    ------------------------------------------------------------------------------
```

T

he following information is displayed if the example number the user entered is 2:

```
Ruijie#ntp help

---------------------------------- Example Menu ----------------------------------
1. NTP client/server mode configuration example
2. NTP client/server ID authentication mode configuration example

------------------------------------------------------------------------------
Please choose the number you want to view (Press the ESC to exit):2

--------------------------- Configuration Requirements ---------------------------
Synchronize the clock of newly-purchased deviceB based on deviceA and set the ID
authentication for the communication between the two devices. Set the deviceA IP
address 1.1.1.1 and clock layer 12.

------------------------------ Configuration Steps -------------------------------
1. NTP server configuration
DeviceA(config)#ntp authenticate
DeviceA(config)#ntp authentication-key 5 md5 helloword
DeviceA(config)#ntp trusted-key 5
//Configure the NTP ID authentication.

DeviceA(config)#interface vlan 1
DeviceA(config-vlan 1)#ip address 1.1.1.1 255.255.255.0
DeviceA(config-vlan 1)#exit
//Configure the IP address of the server.

DeviceA(config)#ntp master 12
//Set the local clock as reference clock(clock layer 12) and enable the ntp
server function. The number of clock layer determines the clock accuracy, in the
range of 1-15 (default: 8). Smaller layer means the higher accuracy.
DeviceA(config)#show clock
//View cunrrent time of the server.

2. NTP client configuration
DeviceB(config)#ntp authenticate
DeviceB(config)#ntp authentication-key 5 md5 helloword
DeviceB(config)#ntp trusted-key 5
//Configure the NTP ID authentication, the trusted-key must be the same as the
server.

DeviceB(config)#show clock
//View the client time before synchronizaton.
DeviceB(config)#ntp server 1.1.1.1 key 5
//Designate the deviceA as the clock source of deviceB (namely server). Enable
the ntp client function and specify the key ID used to communicate with server.
DeviceB(config)#view ntp
//View whether the synchronization is successful.
------------------------------------------------------------------------------
```

Note:

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related

Command	Description

Commands

view ntp	Shows the configurations and running status information about NTP modules.

Platform Description N/A

ntp help

Use this command to show information about command examples beginning with the keyword **ntp**.

ntp help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global or interface configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure misleading.
In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples The following is the command output in global configuration mode:
English interface:

```
Ruijie(config)#ntp help

Examples:
--------------------------------------------------------------------------------
>ntp master 12

Set the local clock as the NTP master clock with the clock layer 12. Enable the
ntp server function.
--------------------------------------------------------------------------------
>ntp server 1.1.1.1

Specify the NTP server as 1.1.1.1 and enable the ntp client function.
--------------------------------------------------------------------------------
>ntp update-calendar

Enable the regular update of NTP hardware clock.
--------------------------------------------------------------------------------
```

The following is the command output in interface mode:
English interface:

```
Ruijie(config-GigabitEthernet 0/4)#ntp help

Example:
--------------------------------------------------------------------------------
>ntp disable

Prohibit recieving the NTP packets on this interface.
--------------------------------------------------------------------------------
```

Note:

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands	Command	Description
	ntp help	Shows typical configuration of NTP modules.

Platform Description N/A

ntp server help

Use this command to view information about command examples beginning with the keyword **ntp server**.

ntp server help

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure and misleading.

In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples The following is the command output:

English interface:

```
Ruijie(config)#ntp server help

Examples:
------------------------------------------------------------------------------
>ntp server 1.1.1.1 source gigabitEthernet 0/2

Specify a NTP server, and a source interface on which the NTP packets are sent.
1.1.1.1: IP address of the NTP server;    gigabitEthernet 0/2: source interface;
------------------------------------------------------------------------------
>ntp server 2000::2 key 4

Specify a NTP server and an encryption key used to communicate with corresponding
server.
2000::2: IP address of the NTP server;
4: encryption key used to communicate with corresponding server;
------------------------------------------------------------------------------
```

Note:

You can use the **language {chinese | english}** command in privileged mode to switch interfaces

Related Commands

Command	Description
ntp help	Shows typical configuration of NTP modules.

Platform Description N/A

ntp access-group help

Use this command to show information about command examples beginning with the keyword **ntp access-group**.

ntp access-group help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure and misleading.

In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples The following is the command output in global configuration mode:

English interface:

```
Ruijie(config)#ntp access-group help

Examples:
------------------------------------------------------------------------------
>ntp access-group peer 1

The peer devices in the IP ACL1 can perform the time request, query control and
time synchronization to local device.
------------------------------------------------------------------------------
>ntp access-group server-only lin

The peer device in ACL lin can only request time to local device.
------------------------------------------------------------------------------
```

Note:

You can use the **language {chinese | english}** command in privileged mode to switch interfaces.

Related Commands

Command	Description
ntp help	Shows typical configuration of NTP modules.

Platform Description N/A

ntp authencation-key help

Use this command to view information about command examples beginning with the keyword **ntp authentication-key**.

ntp authentication-key help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Currently, if you add the question mark (?) when entering a configuration command, the description about the configuration of the next keyword or parameter will be displayed after the question mark (?). However, the description may be obscure and misleading.

In this case, configuration examples about common and key configuration commands in Chinese can improve the configuration accuracy and efficiency, help you understand configuration effects, and optimize the configuration experience.

Configuration Examples The following is the command output in global configuration mode:

English interface:

```
Ruijie(config)#ntp authentication-key help

Examples:
------------------------------------------------------------------------------
>ntp authentication-key 6 md5 wooop

Configure a global NTP authentication key for the NTP service.
6: key ID;                    wooop: key string;
------------------------------------------------------------------------------
>ntp authentication-key 2 md5 024747 7

Configure a global NTP authentication key for the NTP service, which is
cipher-text.
2: key ID;                    024747: key string;
7: encapsulation type;
------------------------------------------------------------------------------
```

Note:

You can use the **language** { **chinese** | **english** } command in privileged mode to switch interfaces.

Related Commands

Command	Description
ntp help	Shows typical configuration of NTP modules.

Platform Description N/A

show ntp server

Use this command to show information about the NTP server.

show ntp server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode This command can be performed in any modes.

Usage Guide N/A

Configuration Examples The following is the command output:

```
Ruijie#show ntp server
ntp server: maxnum 20, have assigned 4
ntp-server                              source    keyid        prefer  version
--------------------------------------  --------  -----------  ------  -------
1.1.1.1                                 None      1            FALSE   3
1.1.2.4                                 Gi0/4     None         FALSE   2
192.168.23.41                           None      None         FALSE   3
192.168.4.11                            None      None         FALSE   3
```

Related Commands

Command	Description
ntp help	Shows typical configuration of NTP modules.

Platform Description N/A

view ntp

Use this command to view the configurations and running status about NTP modules.

view ntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode This command can be performed in any modes.

Usage Guide Currently, you can use two commands on the CLI to respectively show the configurations and the status information. For the required information of a specific state, you must use several related commands, which is complex. For simplification, it is necessary to show the status information together with the related configurations.

Configuration Examples The following is the command output:

```
Ruijie#view ntp

ntp server service:       Disabled
ntp server stratum:       16
ntp client service:       Enabled
ntp authenticate:         Enabled
ntp authentication-key:   7, 11, 20
ntp trusted-key:          2, 3
ntp update-calendar:      Disabled
ntp access-group:         None
ntp disable on interface: Gi0/3

last synchronized:       Successful
reference clock:         192.168.64.221
reference clock stratum: 12
reference time:          00:06:50.000 UTC Sat, Jan 1, 2000
current time:            00:08:24.000 UTC Sat, Jan 1, 2000
More information, refer to: show ntp status

ntp server: maxnum 20, have assigned 4
ntp-server                              source    keyid        prefer  version
--------------------------------------  --------  -----------  ------  -------
1.1.1.1                                 None      1            FALSE   3
1.1.2.4                                 Gi0/4     None         FALSE   2
192.168.23.41                           None      None         FALSE   3
```

```
...
More information, refer to: show ntp server
```

Related Commands

Command	Description
ntp help	Shows typical configuration of NTP modules.

Platform Description N/A

SNTP Commands

sntp enable

Use this command to enable the Simple Network Time Protocol (SNTP). Use the **no** form of this command to restore the default value **Disable**.

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 This command shows SNTP parameters.

Configuration Examples

```
Ruijie(config)# sntp enable
```

Related Commands

Command	Description
show sntp	Shows the SNTP configuration.
clock update-calendar	Synchronizes the software clock with the hardware clock.
clock set	Sets the software clock.

Platform Description N/A

sntp interval

Use this command to set the interval for the SNTP Client to synchronize its clock with the NTP/SNTP Server.

sntp interva *seconds*

no sntp interval

Parameter

Parameter	Description

Description

seconds	Synchronization interval in the range 60 to 65535 seconds

Defaults The interval is 1800 seconds by default.

Command Mode Global configuration mode

Usage Guide The **show sntp** command shows SNTP parameters.


Caution The interval will take effect after the **sntp enable** command is executed.

Configuration Examples

```
Ruijie(config)# sntp interval 3600
```

Related Commands

Command	Description
sntp enable	Enables SNTP.
show sntp	Shows the SNTP configuration.
clock update-calendar	Synchronizes the software clock with the hardware clock.

Platform Description N/A

sntp server

Use this command to set the SNTP server. You can configure the SNTP server as the public NTP server on the Internet, since SNTP is completely compatible with NTP.

sntp server *ip-address*

no sntp server

Parameter Description

Parameter	Description
ip-address	IP address of the NTP/SNTP server.

Defaults No NTP/SNTP server is configured by default.

Command Mode Global configuration mode

Usage Guide The **show sntp** command shows SNTP parameters.

Configuration Examples

```
Ruijie(config)# sntp server 192.168.4.12
```

Related Commands

Command	Description
show sntp	Shows the SNTP configuration status.
sntp enable	Enables SNTP.

Platform Description N/A

show sntp

Use this command to show SNTP parameters.

show sntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide This command shows SNTP parameters.

Configuration Examples

```
Ruijie# show  sntp
SNTP state                : Enable
SNTP server               : 192.168.4.12
SNTP sync interval    : 60
Time zone                 : +8
```

Related Commands

Command	Description
sntp enable	Enables SNTP.
show sntp	Shows the SNTP parameters.

Platform Description N/A

sntp help

Use this command to show the typical configuration of the SNTP module.

sntp help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide For the current operation of the CLI, commands are executed one by one. CLI presentation lacks typical replicable configuration examples for the configuration and deployment of a specific functional module. Therefore, you can only obtain the configuration help by other means (such as reading related manuals and consulting frontline engineers)

In this case, showing typical configurations on the CLI provides the help information about the quick basic deployment of a certain function for users, increasing CLI usability.

Configuration Examples The folloiwng is the output of this command in privileged mode:

English interface:

```
Ruijie#sntp help

-------------------------- Configuration Requirements --------------------------
A school has recently purchased a device, and the administrator expects to
enable clock synchronization. The synchronization interval shall be 1h, and the
IP address of SNTP server shall be 1.1.1.1.

------------------------------ Configuration Steps  ------------------------------
1. Configure basic parameters
Ruijie(config)#sntp server 1.1.1.1
//Specify the SNTP server
Ruijie(config)#sntp interval 3600
//Configure the interval for SNTP synchronization, with unit being second and
range being 60-65535. The default value is 1800.
Ruijie(config)#clock timezone tz 8
//Configure local time zone (name: tz) from the range of -23 to 23; negative
number represents west zone, and positive number represents east zone. The
default value is 0.

2. Enable SNTP service
Ruijie(config)#sntp enable
//Enable SNTP service. Execute this command to trigger clock synchronization
instantly without waiting for timed synchronization.

3. View SNTP status
Ruijie(config)#view sntp
--------------------------------------------------------------------------------
```

Note:

You can the **language** { **chinese | english** } command in global configuration mode to switch interfaces.

Related Commands	Command	Description
	view sntp	Shows the configuration and running status about SNTP module.

Platform Description N/A

view sntp

Use this command to show the configuration and running status information about the SNTP module.
view sntp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode This command can be performed in any modes.

Usage Guide Currently, you can use two commands on the CLI to respectively show the configurations and the status information. For the required information of a specific state, you must use several related commands, which is complex. For simplification, it is necessary to show the status information together with the related configurations.

Configuration Examples The following is output of this command:

```
Ruijie#view sntp

SNTP state:             Enabled
SNTP server:            1.1.1.1
SNTP sync interval:     3600s
Time zone:              8(east)
Last synchronized:      successed

Function characteristics      Default value
-------------------------     -----------------
SNTP state                    Disabled
SNTP server                   None
SNTP sync interval            1800s
Time zone                     0
```

Related Commands	Command	Description
	sntp help	Shows the typical configuration of the SNTP module.

Platform Description N/A

UDP-Helper Module Commands

ip forward-protocol

Use this command to configure the User Datagram Protocol (UDP) port to enable relay forwarding. Use the **no** form of this command to disable forwarding on the UDP port.

ip forward-protocol udp [*port* | **tftp** | **domain** | **time** | **netbios-ns | netbios-dgm** | **tacacs**]

no ip forward-protocol udp [*port* | **tftp** | **domain** | **time** | **netbios-ns** | **netbios-dgm** | **tacacs**]

Parameter Description

Parameter	Description
port	Port where relay forwarding is enabled. If this parameter is not specified, the broadcast packet from the ports 69, 53, 37, 137, 138, and 49 will be forwarded by default.
tftp	Specified by Trivial File Transfer Protocol(69). If this parameter is specified, the broadcast packet from port 69 is relayed and forwarded.
domain	Specified by Domain Name System(53). If this parameter is specified, the broadcast packet from port 53 is forwarded.
time	Specified by Time service(37). If this parameter is specified, the broadcast packet from port 37 is forwarded.
netbios-ns	Specified by NetBIOS Name Service(137). If this parameter is specified, the broadcast packet from port 137 is forwarded.
netbios-dgm	Specified by NetBIOS Datagram Service(138). If this parameter is specified, the broadcast packet from port 138 is forwarded.
tacacs	Specified by TAC Access Control System(49). If this parameter is specified, the broadcast packet from port 49 is forwarded.

Defaults No UDP port for forwarding is configured by default.

Command Mode Global configuration mode

Usage Guide Enabling UDP-Helper means to forward the broadcast packet of the UDP ports 69, 53, 37, 137, 138, and 49 without any additional configuration, by default.

Configuration Examples

Ruijie(config)# ip forward-protocol udp *134*

Related Commands

Command	Description
udp-helper enable	Enables the forwarding of the UDP broadcast packet.
ip forward-protocol	Configures the UDP port to enalbe relay forwarding.

Platform Description

This command is supported on RGOS10.1 and later versions.

ip helper-address

Use this command to configure the destination server which the UDP broadcast packet will be forwarded to. Use the **no** form of this command to delete the destination server.

ip helper-address *address*

no ip helper-address [***address***]

Parameter Description

Parameter	Description
address	IP address of the destination server in the dotted decimal format. Each interface supports up to 20 server addresses.

Defaults

N/A

Command Mode

Interface configuration mode

Usage Guide

Up to 20 destination servers can be configured on an interface. If the destination server is configured on an interface and UDP-Helper is enabled, the broadcast packet of the specified port received from this interface will be sent to the destination server configured on this interface in unicast form.

Use the **no ip helper-address** command to remove the destination server.

Configuration Examples

The following is an example of configuring the destination server where the UDP broadcast packet will be forwarded to.

Ruijie(config-if)# **ip helper-address** *192.168.100.1*

Related Commands

Command	Description
ip forward-protocol	Enables the forwarding function on the UDP port.

Platform Description This command is supported on RGOS10.1 and later versions.

udp-helper enable

Use this command to enable relay forwarding for the UDP broadcast packet. Use the **no** form of thiscommand to disable this function.
This function is disabled by default.
udp-helper enable
no udp-helper enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The relay and forwarding of the UDP broadcast packet is disabled by default.

Command Mode Global configuration mode

Usage Guide Enable the forwarding function of UDP-Helper. The UDP broadcast packets from the port 69, 53, 37, 137, 138, and 49 are relayed and forwarded by default.

Configuration Examples The following example of enables the UDP forwarding function.

```
Ruijie(config)# udp-helper enable
```

Related Commands

Command	Description
ip forward-protocol	Enables the forwarding function on the UDP port..

Platform Description This command is supported on RGOS10 and later versions.

URPF Commands

ip verify unicast source reachable-via (Global configuration mode)

Use this command to enable the Unicast Reverse Path Forwarding (URPF) feature in global configuration mode. Use the no form of this command to disable the URPF function or remove the URPF options.

ip verify unicast source reachable-via rx

no ip verify unicast

Parameter Description

Parameter	Description
rx	URPF check in strict mode. In strict mode, the the ingress port of a packet must be matched with the egress port of the forwarding entry found in the forwarding table according to the source address of the IP packet..

Defaults The URPF function is disabled by default.

Command Mode Global configuration mode

Usage Guide The URPF function determines the packet validity by checking whether the route to the source address exists in the forwarding table. If no forwarding entry is matched, the packet is invalid.

Enabling the URPF function in global configuration mode indicates to enable URPF check for the received packets on all interfaces.

1. The configuration of the URPF function in global configuration mode only takes effect on the S8600 series switches after the MPLS line card is inserted. After the URPF function takes effect, URPF check is enabled for IPv4 packets.

2. The URPF function configured in global configuration mode URPF function can only be enabled in strict mode. However, if the equal-cost route is matched, the mode switches to loose mode.

3. In global configuration mode, the URPF function does not support the URPF check using the default route.

4. The URPF function cannot be configured in global configuration mode and in interface configuration mode at the same time.

5. Note that it is not recommended to configure URPF globally if the S8600 series devices are directly connected to users' network segments. The URPF check fails and the packets are discarded if the S8600 series devices did not learn the ARP entry of a directly-connected user before packets

forwarding.

Configuration Examples The following example enables the URPF function globally:

```
Ruijie(config)# ip verify unicast source reachable-via rx
```

Related Commands

Command	Description
show ip urpf	Shows the URPF information.

Platform Description

ip verify unicast source reachable-via (Interface configuration mode)

Use this command to enable the URPF function in interface configuration mode. Use the **no** form of this command to disable the URPF function or remove the URPF options.

ip verify unicast source reachable-via {**rx** | **any**} [**allow-default]** [*acl_name*]

no ip verify unicast

Parameter Description

Parameter	Description
rx	URPF check in strict mode. In strict mode, the ingress port of a packet must be matched with the egress port of the forwarding entry found in the forwarding table according to the source address of the IP packet.
any	URPF check in loose mode. In loose mode, the only requirement of forwarding a packet is to find its forwarding entry in the forwarding table according to the source address of the packet.
allow-default	(Optional) Allows the default route in URPF check.
acl_name	(Optional) Sets the Access Control List (ACL) number in the range: 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)

Defaults The URPF function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The URPF function determines the packet validity by checking whether the route to the source address exists in the forwarding table. If no forwarding entry is matched, the packet is invalid.

Enabling URPF function in interface configuration mode indicates to enable 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 failed to pass the URPF check are discarded. With ACL (acl-name) configured, the ACL matching continues when the routing fails. The packets will be discarded if the ACL is nonexistent or the deny Access Control Entry (ACE) is matched; otherwise, if the permit ACE is matched, the packets will be forwarded.

1、After this command is used, the S5700 V2.x switch and the S8600 series switches will enable the URPF check on both IPv4 and IPv6 packets, and the routers will enable the URPF check on IPv4 packets.

2. The switch products support the URPF function only on the S5700 V2.x switch and the routed port and Layer 3 AP associated with category B line cards of the S8600 series. The restrictions are as follows:

The URPF function does not support the function of associating ACL options.

The URPF function does not support the URPF check using an IPv6 route with a 65-to-127 bit prefix.

After the URPF function is enabled on interfaces, the URPF check will be enabled on all packets received on the physical ports corresponding to these interfaces, expanding the range of URPF check. The typical application scenario is that the URPF check will be implemented on the packet if it is received from the physical port of a Tunnel port. In this case, it is recommended to enable the URPF check prudently.

After the URPF function is enabled, the forwarding capacity of routers is reduced by half.

URPF strict mode will switch to loose mode if the packet received on an interface matches the equal-cost route during URPF check.

The URPF function cannot take effect on interfaces of the S8600 series switches after the MPLS line card is inserted.

3. URPF function cannot be configured in global configuration mode and in interface configuration mode at the same time.

Configuration Examples

The following example checks the URPF function of the received packets in strict mode on GigabitEthernet 0/21 with no need of the default route.

```
Ruijie(config)# interface gigabitEthernet0/21
Ruijie(config-if)# ip verify unicast source reachable-via rx
```

Related Commands

Command	Description
show ip urpf	Shows the URPF information.

Platform Description

This command is supported on all router products,

ip verify urpf drop-rate compute interval

Use this command to set the interval at which the URPF packet loss rate is computed. Use the **no**

form of this command to restore the default value.

ip verify urpf drop-rate compute interval *seconds*

no ip verify urpf drop-rate compute interval

Parameter Description

Parameter	Description
seconds	Sets the interval at which the URPF packet loss rate is computed in seconds. In the range from 30 to 300, the default value is 30 seconds.

Defaults The default value is 30 seconds.

Command Mode Global configuration mode

Usage Guide The URPF drop-rate compute interval is configured in global configuration mode. It is applicable to the global URPF drop-rate compute and that of interfaces enabled with the URPF function.

Configuration Examples The following example sets the URPF drop-rate compute interval as 1 minute:

```
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 This command is supported on all router products

ip verify urpf drop-rate notify

Use this command to enable the URPF drop-rate information monitoring. Use the **no** form of this command to disable this function.

ip verify urpf drop-rate notify

no ip verify urpf drop-rate notify

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Interface configuration mode

Mode

Usage Guide This command enables URPF drop-rate information monitoring to notify the user of the URPF packet drop rate information using Syslog or Trap, facilitating network monitoring.

Configuration Examples The following example enables the URPF drop-rate information monitoring on GigabitEthernet 0/21.

```
Ruijie(config)# interface gigabitEthernet0/21
Ruijie(config-if)# ip verify urpf drop-rate notify
```

Related Commands

Command	Description
ip verify urpf drop-rate compute interval	Sets *urpf drop-rate compute interval*.
ip verify urpf drop-rate notify hold-down	Sets *urpf drop-rate notify hold-down*.
ip verify urpf notification threshold	Sets *urpf notification threshold*.

Platform Description This command is supported on all router products

ip verify urpf drop-rate notify hold-down

Use this command to configure *urpf drop-rate notify hold-down*. Use the **no** form of this command to restore the default value.

ip verify urpf drop-rate notify hold-down *seconds*

no ip verify urpf drop-rate notify hold-down

Parameter Description

Parameter	Description
seconds	Sets urpf drop-rate notify hold-down in seconds. The range is from 30 to 300 and the default value is 300 seconds.

Defaults The default value is 300 seconds.

Command Mode Global configuration mode

Usage Guide The parameter *urpf drop-rate notify hold-down* is configured in global configuration mode. It is applicable to the global URPF drop-rate warning and that of interfaces enabled with the URPF function.

Configuration Examples The following example configures *urpf drop-rate notify hold-down* to 1 minute:

```
Ruijie(config)# ip verify urpf drop-rate notify hold-down 60
```

Related Commands

Command	Description

ip verify urpf drop-rate compute interval	Configures *urpf drop-rate compute interval*.
ip verify urpf drop-rate notify	Enables the URPF drop-rate information monitoring.
ip verify urpf notification threshold	Configures the *urpf notification threshold*.

Platform Description This command is supported on all router products

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 value.

ip verify urpf notification threshold *rate-value*

no ip verify urpf notification threshold

Parameter Description

Parameter	Description
rate-value	Sets the URPF drop-rate threshold in packets per second (pps). The range is 0 to 4294967295. The default value is 1000 pps.

Defaults The default value is 1000 pps.

Command Mode Interface configuration mode

Usage Guide The threshold **0** indicates that once a dropped packet is monitored due to the URPF check, the notification is sent.

You can adjust the drop-rate threshold value according as required.

Configuration Examples The following example sets the URPF drop-rate threshold as 10 pps on GigabitEthernet 0/21.

```
Ruijie(config)# interface gigabitEthernet0/21
Ruijie(config-if)# ip verify urpf drop-rate notify
Ruijie(config-if)# ip verify urpf notification threshold 10
```

Related Commands

Command	Description
ip verify urpf drop-rate compute interval	Configures *urpf drop-rate compute interval*.
ip verify urpf drop-rate notify	Enables the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Configures *urpf drop-rate notify hold-down*.

Platform Description This command is supported on all router products

snmp-server enable traps

Use this command to enable the URPF Trap notification if the URPF drop-rate exceeds the threshold. Use the **no** form of this command to disable this function.

snmp-server enable traps urpf

no snmp-server enable traps urpf

Parameter Description

Parameter	Description
urpf	Enables the URPF Trap notification.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide By default, when the URPF drop-rate exceeds the threshold, it auto-notifies the user using Syslog. However, after this command is configured, the URPF Trap notification is allowed.

Configuration Examples The following example enables the Trap notification when the URPF drop-rate exceeds the threshold**.**

```
Ruijie(config)# snmp-server enable traps urpf
```

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host.
ip verify urpf drop-rate compute interval	Configures the URPF drop-rate compute interval.
ip verify urpf drop-rate notify	Configures the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Configures the URPF drop-rate warning interval.
ip verify urpf notification threshold	Configures the URPF drop-rate threshold.

Platform Description This command is supported on all router products

snmp-server host traps

Use this command to specify the Simple Network Management Protocol (SNMP) host (NMS indicates Network Management System) to receive the URPF Trap message in global configuration mode. Use the **no** form of this command to remove the specified SNMP host.

snmp-server host { *host-addr* | **ipv6** *ipv6-addr* } **traps** *community-string* [**urpf**]

no snmp-server host { host-addr | ipv6 ipv6-addr } **traps** *community-string*

Parameter Description

Parameter	Description
host-addr	SNMP host address
ipv6-addr	SNMP IPv6 address
community-string	Community string or username (Version3)
urpf	URPF Trap

Defaults No SNMP host is specified by default.
If the trap type is not specified, all Trap types are included.

Command Mode Global configuration mode

Usage Guide Use this command and the **snmp-server enable traps** command to send the URPF Trap messages to the specified NMS.

Configuration Examples The following example specifies the SNMP host 192.168.12.219 to receive the URPF Trap message.

Ruijie(config)# **snmp-server host** *192.168.12.219* traps **public urpf**

Related Commands

Command	Description
snmp-server enable traps	Enables to send the Trap message.
ip verify urpf drop-rate compute interval	Configures *urpf drop-rate compute interval*.
ip verify urpf drop-rate notify	Configures the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Configures *urpf drop-rate notify hold-down*.
ip verify urpf notification threshold	Configures *urpf notification threshold*.

Platform Description This command is supported on all router products

show ip urpf

Use this command to show the URPF configuration and statistics.

show ip urpf [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface *interface-name*	Shows the configurations and statistics on the specified interface.

Defaults N/A

Command Mode Privileged mode

Usage Guide With no interface specified, the global configurations and statistics of all interfaces are shown.

Configuration Examples The following example shows the URPF configuration and statistics on GigabitEthernet 0/21.

```
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
```

Related Commands

Command	Description
ip verify unicast source reachable-via	Enables the URPF function.
ip verify urpf drop-rate compute interval	Configures *urpf drop-rate compute interval*.
ip verify urpf drop-rate notify hold-down	Configures *urpf drop-rate notify hold-down*.
ip verify urpf notification threshold	Configures *urpf notification threshold*.
clear ip urpf	Clears the URPF statistics.

Platform Description This command is supported on all router products

clear ip urpf

Use this command to clear the URPF statistics about the dropped packets.

clear ip urpf [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface *interface-name*	Clears the statistics on the specified interface.

Defaults N/A

Command Mode Privileged mode

Usage Guide With no interface specified, the statistics of all interfaces are cleared.

Configuration Examples The following example clears the statistics about URPF drop-rate on the specified interface GigabitEthernet 0/21:

```
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
Ruijie# clear ip urpf interface gigabitEthernet0/21
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 0
Number of drop-rate notification counts in this interface is 0
```

Related Commands

Command	Description
showip urpf	Shows the URPF configurations and statistics.

Platform Description This command is supported on all router products

IPFIX Commands

cache

Use this command to set cache parameters in IPFIX flow aggregation configuration mode. Use the **no** form of this command to restore the default value.

cache { **entries** number | **timeout** { **active** minutes | **inactive** seconds} }

no cache { **entries** | **timeout** { **active** | **inactive** } }

Parameter Description

Parameter	Description
entries *number*	Number of entries allowed in the aggregation cache. The range is 1024 to 524288.
timeout	Aging time of aggregation entries, including active aging time and inactive aging time.
active *minutes*	Active aging time in minutes, that is the time an active entry exists in the aggregation cache before the entry is exported or deleted. The range is 1 to 60 minutes. The default value is 30 minutes.
inactive *seconds*	Inactive aging time in seconds. An aggregation entry is aged if the flow record of the entry is not detected within the inactive aging time. The range is 10 to 600 seconds. The default value is 15 seconds.

Defaults

The number of aggregation entries is 4096 by default.
Active aging time is 30 minutes by default.
Inactive aging time is 15 seconds by default.

Command Mode

IPFIX flow aggregation configuration mode

Usage Guide

The IPFIX must have been enabled globally before this command is used, and the number of entries must be configured before aggregation mode is enabled. If aggregation mode has been enabled, the configuration does not take effect immediately until it restarts.

Configuration Examples

The following example shows how to configure the number of cache entries, active aging time and inactive aging time in flow aggregation mode. Besides, when the system is busy, the accuracy of actual output time will be influenced， which leads to a 10-35 deviation.

```
Ruijie(config)# ip flow-aggregation cache protocol-port
Ruijie(config-flow-cache)# cache entries 2046
Ruijie(config-flow-cache)# cache timeout inactive 199
```

```
Ruijie(config-flow-cache)# cache timeout active 45
Ruijie(config-flow-cache)# enabled
```

Related Commands

Command	Description
show ip flow cache	Shows the flow statistics information in the current cache in main mode
show ip flow cache aggregation	Shows the flow statistics information in flow aggregation mode

Platform Description N/A

clear ip flow-cache

Use this command to clear flow statistics in privileged mode.

clear ip flow-cache

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide Global IPFIX must have been enabled before this command is used. You can use the **show ip flow cache** command to show current IP flow statistics information, and the **show ip flow cache** command to clear such information.

Configuration Examples The following example shows how to clear the current IP flow statistics information.

```
Ruijie# clear ip flow-cache
```

Related Commands

Command	Description
show ip flow cache	Shows the flow statistics information in the main cache.
show ip flow cache aggregation	Shows the flow statistics information of corresponding flow aggregation mode.

Platform Description N/A

clear ip flow stats

Use this command to remove the flow statistics information in privileged EXEC configuration mode.
clear ip flow stats

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged mode

Usage Guide IPFIX must have been enabled globally before this command is enabled. You can use **show ip cache flow** command to show the statistics information of the current IP flows, and use the **clear ip flow stats** command to clear the current protocol flow statistics information.

Configuration Examples The following example shows how to clear the protocol statistics information.

```
Ruijie# clear ip flow stats
```

Related Commands

Command	Description
show ip flow cache	Shows the flow statistics information in the current cache in main mode.

Platform Description N/A

enabled (aggregation cache)

Use this command to enable the flow aggregation function in IPFIX flow aggregation configuration mode. Use the **no** form of this command to disable the flow aggregation function.
enabled
no enabled

Parameter Description

Parameter	Description
N/A	N/A

Defaults All aggregation modes are disabled by default.

Command IPFIX flow aggregation configuration mode

Mode

Usage Guide IPFIX must have been enabled globally before this command is used is used.

Configuration Examples The following example shows how to enable the protocol-port aggregation function.

```
Ruijie(config)# ip flow-aggregation cache protocol-port
Ruijie(config-flow-cache)# enabled
```

The following example shows how to disable the protocol-port aggregation function.

```
Ruijie(config)# ip flow-aggregation cache protocol-port
Ruijie(config-flow-cache)# no enabled
```

Related Commands

Command	Description
ip flow-aggregation cache	Enters IPFIX flow aggregation configuration mode.
cache	Sets cache parameters.
export destination (**aggregation cache**)	Exports flow aggregation records in flow aggregation configuration mode to the destination.
mask (**IPv4**)	Specifies the prefix code of source or destination address for prefix aggregation mode.
export destination (**aggregation cache**)	Shows the flow aggregation statistics information of one flow aggregation mode.

Platform Description N/A

export

Use this command to export flow aggregation records in IPFIX flow aggregation mode. Use the **no** form of this command to delete a pair of destination address and destination port, or restore some parameters to their default values.

export { **destination** [*ip-address* | *hostname*] *udp-port* [**vrf** *vrf-name*] } | **template** [**refresh-rate** *packets* | **timeout-rate** *minutes*]

no export { **destination** [*ip-address* | *hostname*] *udp-port*} | **template** [**refresh-rate** | **timeout-rate**]

Parameter Description

Parameter	Description
destination *ip-address* | *udp-port*	Specifies the destination address and destination port to which the flow statistics information is exported.
template	Enables the template keywords refresh-rate and timeout-rate, which configures template export.

refresh-rate *packets*	(Optional) Specifies the frequency of template retransmission in packets. The range is 1 to 600 packets. The default value is 20 packets.
timeout-rate *minutes*	(Optional) Specifies the frequency of template retransmission in minutes. The range is 1 to 1000 minutes. The default value is 10 minutes.
version [**9** | **10**]	Exports the version 9 or 10 template.
destination *ip-address* | *udp-port*	Specifies the destination address and destination port to which the flow statistics information is exported.

Defaults No destination address or destination port is set by default.
The refresh-rate parameter is set to 20 packets and the timeout-rate parameter is to 10 minutes by default.
The version parameter is set to 10 by default.

Command Mode IPFIX flow aggregation configuration mode

Usage Guide IPFIX must have been enabled globally before this command is used. You can use the **export destination** command to configure up to two destinations for each flow aggregation mode.

Configuration Examples The following example shows how to configure two output destinations for the flow aggregation mode of **protocol-port**.

```
Ruijie(config)# ip flow-aggregation cache protocol-port
Ruijie(config-flow-cache)# export destination 10.41.41.1 9992
Ruijie(config-flow-cache)# export destination 172.16.89.1 9992
Ruijie(config-flow-cache)# enabled
```

The following example shows how to configure the packet output format and template refresh rate for the protocol-port flow aggregation mode.

```
Ruijie(config)# ip flow-aggregation cache protocol-port
Ruijie(config-flow-cache)# export template refresh-rate 100
Ruijie(config-flow-cache)# export template timeout-rate 120
Ruijie(config-flow-cache)# enabled
```

Related Commands

Command	Description
ip flow-aggregation cache	Enters IPFIX flow aggregate configuration mode.
cache	Configures cache parameters.
export destination (**aggregation cache**)	Exports flow aggregation records to the destination in flow aggregation configuration mode.
mask (**IPv4**)	Specifies the prefix code of source or destination address for prefix aggregation

	mode.
show ip flow cache aggregation	Shows the flow aggregation statistics information of one flow aggregation mode.

Platform Description N/A

flow-sampler filter

Use this command to take sample and filter specified messages in interface configuration mode,. Use the **no** form of this command to restores the default configuration.

flow-sampler *packet-name* **filter** *acl-name*

no flow-sampler

Parameter Description

Parameter	Description
acl-name	Name or ID of the created ACL. If the acl-name is 0, all messages from this port will be taken sample.
packet-name	Sampling rate, in the range of 255 to 16777215.

Defaults The sampling rate is 1/255 for all message from this port by default.

Command Mode Interface configuration mode

Usage Guide Before using this command, ensure that the configured acl-name exists or is set to 0.
Routers only support the 1:1 sampling rate.

Configuration Examples The following example shows how to configure the filtering mechanism on interface 1/1.

```
Ruijie# config terminal
Ruijie(config)# interface ethernet 1/1
Ruijie(config-if)# flow-sample 500 filter acl1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip flow-aggregation cache

Use this command to enable flow aggregation mode and enter flow aggregation configuration mode

in global configuration mode. Use the **no** form of this command to disable flow aggregation mode, which is equivalent to the **no enabled** command in flow aggregation command configuration mode.

ip flow-aggregation cache { **destination-prefix | destination-prefix-tos | prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}

no ip flow-aggregation cache { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }

Parameter Description

Parameter	Description
destination-prefix	Destination-prefix flow aggregation mode
destination-prefix-tos	Destination-prefix-tos flow aggregation mode
prefix	Prefix flow aggregation mode
prefix-port	Prefix-port flow aggregation mode
prefix-tos	Prefix-tos flow aggregation mode
protocol-port:	Protocol-port flow aggregation mode
protocol-port-tos	Protocol-port-tos flow aggregation mode
source-prefix	Source-prefix flow aggregation mode
source-prefix-tos	Source-prefix-tos flow aggregation mode

Defaults N/A

Command Mode Global configuration mode

Usage Guide IPFIX must have been enabled globally before this command is used. The **export destination** command can configure at most two destinations at the same time. Flow aggregation mode with the suffix of **tos** indicates that the egress flow records contain the **tos** field, an 8-bit field of the IP header indicating the quality of service in transmission.

The following rules apply to the configuration of masks of source and destination addresses.

The mask of source address can be configured only in aggregation modes of **prefix**, **prefix-port**, **prefix-tos**, **source-prefix**, and **source-prefix-tos**.

The mask of destination address can be configured only in aggregation modes of **prefix**, **prefix-port**, **prefix-tos**, **destination-prefix**, and **destination-prefix-tos**.

The mask cannot be configured in non-prefix flow aggregation modes.

To enable flow aggregation mode, you must use the **enabled** command in corresponding flow aggregation configuration mode. The **no enabled** command disables flow aggregation mode, but the original values of parameters remain unchanged.

Configuration Examples The following example shows how to set the mask of destination address to **0xFFFF0000** for **destination-prefix** flow aggregation mode.

```
Ruijie(config)# ip flow-aggregation cache destination-prefix
Ruijie(config-flow-cache)# mask destination minimum 16
Ruijie(config-flow-cache)# enabled
```

The following example shows how to set the mask of source address to 0xFFFF0000 for

source-prefix flow aggregation mode.
Ruijie(config)# ip flow-aggregation cache source-prefix
Ruijie(config-flow-cache)# mask source minimum *16*
Ruijie(config-flow-cache)# enabled
The following example shows how to set multiple output destinations for flow aggregation mode of protocol-port.
Ruijie(config)# ip flow-aggregation cache protocol-port
Ruijie(config-flow-cache)# export destination *172.17.24.65 9991*
Ruijie(config-flow-cache)# export destination *172.16.10.2 9991*
Ruijie(config-flow-cache)# enabled

Related Commands

Command	Description
export destination (**aggregation cache**)	Configures the output destination of corresponding flow aggregation records.
enabled (**aggregation cache**)	Enables flow aggregation mode.
mask (**IPv4**)	Specifies the prefix code of source or destination address for prefix aggregation mode.

Platform Description N/A

ip flow-cache entries

Use this command in global configuration mode to specify the number of cache entries in main mode,. Use the **no** form of this command to restore the default value.
ip flow-cache entries *number*
no ip flow-cache entries

Parameter Description

Parameter	Description
number	Number of available cache entries in the range 1024 to 262144. The default value is 65536 (64k).

Defaults The number is set to 65536 (64k) by default.

Command Mode Global configuration mode

Usage Guide Generally, the default entries in the flow records can meet most requirements for collecting flow statistics. You can increase or decrease the number of cache entries for special requirements. The recommended number of entries for the high-speed telecom network is 131072 (128k). You can use the **show ip cache flow** command to view the related information.

64 cache entries can be used and each cache entry is 64 bytes by default. Therefore, 4 MB memory is required by default. When an idle entry is obtained from the queue of idle flow entries, the number of idle entries is checked at first. If there are few idle entries, 30 entries are aged according to the accelerated aging mechanism. If there is only one idle entry, 30 entries are forced to age despite their aging time. In this way, idle entries are always available.

It is not recommend to modify the number of cache entries. In global configuration mode, you can use the **no ip flow-cache entries** command to restore the number of cache entries to its default value. If the global IPFIX is enabled (namely, **ip flow ingress** or **ip flow egress** is configured on a port), the change of the cache entries takes effect until you save the configuration and restart the device.

Configuration Examples The following example shows how to set the number of cache entries in main mode to 131,072 (128k).

```
Ruijie(config)# ip flow-cache entries 131072
```

Related Commands

Command	Description
ip flow ingress	Collects statistics for ingress flows at an interface.
ip flow egress	Collects statistics for egress flows at an interface.
ip flow-cache timeout	Configures the aging time of flow records in cache in main mode.
show ip flow interface	Shows the IPFIX status at an interface.

Platform Description N/A

ip flow-cache timeout

Use this command to set the aging time (including active aging time and inactive aging time) of the IPFIX main cache entries in global configuration mode.

ip flow-cache timeout [**active** *minutes* | **inactive** *seconds*]

no ip flow-cache timeout [**active** | **inactive**]

Parameter Description

Parameter	Description
active *minutes*	(Optional) Active aging time of the main cache entries
inactive *seconds*	(Optional) Inactive aging time of the main cache entries

Defaults Active aging time is 30 minutes by default.

Inactive aging time is 15 seconds by default.

Command Mode Global configuration mode

Usage Guide This command sets the active aging time and the inactive aging time based on the memory size of the current device and the interval for refreshing the IPFIX main cache entries. It is valid only for the aging of the IPFIX main cache entries. When inactive aging occurs, aged IPFIX entries are exported to the aggregation table if aggregation is configured, and statistics are cleared. When inactive aging occurs, the IPFIX data template is exported and delivered to the aggregation table.

When IPFIX samples IPv4 flows, inactive aging is controlled by the flow platform. Therefore, the inactive aging value remains invalid. The flow platform controls inactive aging, and notifies IPFIX to implement inactive aging, while the inactive timer does nothing during this course.

Configuration Examples The following example shows how to configure the active aging time to 20 minutes and inactive aging time to 200 seconds for main caches.

```
Ruijie(config)# ip flow-cache active 20
Ruijie(config)# ip flow-cache inactive 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip flow egress

Use this command to collect the statistics of egress flows in interface configuration mode,. Use the **no** form of this command to disable this function.

ip flow egress

no ip flow egress

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is disabled for each interface by default.

Command Mode Interface configuration mode

Usage Guide Use this command to enable the global IPFIX. The global IPFIX is enabled only when **ip flow egress** or **ip flow ingress** is configured on at least one port.

However, you cannot configure **ip flow egress** and **ip flow ingress** on the same port. The latest configuration overwrites the former configuration, affects newly established flows, but does not affect flows that have been established.

Configuration Examples

The following example shows how to configure the statistics function of egress IP flows on port 1/1.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# ip flow egress
```

Related Commands

Command	Description
ip flow-aggregation cache	Enters IPFIX flow aggregate configuration mode.
snmp-server if-index persist	Ensures the port index remain unchanged when the device is restarted. It is recommanded to enable this function before enabling ipfix.
cache	Configures cache parameters for aggregation modes.
export destination (**aggregation cache**)	Exports flow aggregation records to the destination in flow aggregation configuration mode.
mask (**IPv4**)	Specifies the prefix code of source or destination address for prefix aggregation mode.

Platform Description

N/A

ip flow-export

Use this command to configure the parameters related to exporting the main cache flow in global configuration mode,. Use the **no** form of this command to prohibit this function or restore default value.

ip flow-export { **destination** { { *ip-address* | *hostname* } *udp-port***[vrf** *vrf-name***]** } | **source** { *interface-name* } |**template** { [**refresh-rate** *packets* | **timeout-rate** *minutes* **| options** { [**sample** | **refresh-rate** *packets* | **timeout-rate** *minutes*] }] } }

no ip flow-export { **destination** { { *ip-address* | *hostname* } *udp-port* } | **source** | **template** { [**refresh-rate** | **timeout-rate**] | **options** { [**sample** | **refresh-rate** | **timeout-rate**] } } }

Parameter Description

Parameter	Description
destination { *ip-address* | *hostname udp-port* }	Name or IP address of the collector host to which the output flow records are sent, and the port number on which the collector listens
vrf *vrf-name*	(Optional) VRF name

template	Configure the template for outputting flows.
source *interface-name*	Specifies the configured port IP address as the source IP address for packet output.
refresh-rate *packets*	Sets the frequency of sending the data template and the option template in packets. The range is 1 to 600 packets. The default value is 20.
timeout-rate *minutes*	Sets the frequency of retransmitting the data template and the option template.in minutes. The range is 1 to 1000 minutes. The default value is 10 minutes.
options	Configures export options.
sample	Enables the sampling option export.
refresh-rate *packets*	Sets the frequency of sending options and the option template in packets. The range is 1 to 600 packets. The default value is 20.
timeout-rate *minutes*	Sets the frequency of retransmitting options and the option template.in minutes. The range is 1 to 1000 minutes. The default is 10 minutes.
version [**9** | **10**]	Exports the version 9 or 10 template.

Defaults The destination address and destination port is not set by default.
The refresh-rate is 20 packets by default.
The timeout-rate is 10 minutes by default.
Version 10 template is exported by default.

Command Mode Global configuration mode

Usage Guide After the IPFIX is enabled, you can run the **ip flow-export destination** command to configure the export server of IPFIX flow records. The flow record process software usually runs on the server to process the flow record information exported by the device. This command can set up to two pairs of destination IP address and destination port for exporting flow records to two different servers for redundancy. Generally, you can set two different IP addresses. If you can set the same destination IP address, you must set different destination ports and an alarm occurs and reminds you that the IP addresses of the two servers are the same.

Configuration Examples The following example shows how to set the destination address for the output of flow records in IPFIX main mode.

```
Ruijie(config)# ip flow-export destination 10.42.42.1 9991
```

The following example shows how to set multiple destination addresses for exporting flow records in IPFIX main mode.

```
Ruijie(config)# ip flow-export destination 10.42.42.1 9991
Ruijie(config)# ip flow-export destination 10.0.101.254 9991
```

The following example shows how to set multiple destination addresses for IPFIX main mode.

```
Ruijie(config)# ip flow-export destination 10.42.42.1 9991
Ruijie(config)# ip flow-export destination 10.42.42.2 9992
```

The following example shows how to set the resending rate of data template in main mode.

```
Ruijie(config)# ip flow-export template refresh-rate 100
Ruijie(config)# ip flow-export templa te timeout-rate 60
```

Related Commands

Command	Description
ip flow ingress	Collects statistics of ingress flows at an interface.
ip flow egress	Collects statistics of egress flows at an interface.
ip flow-cache timeout	Configures the aging time of flow records in cache in main mode.
show ip flow cache	Shows the flow statistics information in the current cache.
show ip flow interface	Shows the IPFIX status at each interface.

Platform Description N/A

ip flow ingress

Use this command to collect the statistics of ingress flows in interface configuration mode,. Use the **no** form of this command to disable this function.

ip flow ingress

no ip flow ingress

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is disabled on each port by default.

Command Mode Interface configuration mode

Usage Guide You can use this command to enable IPFIX global statistics function on the device. The global IPFIX is enabled only when the **ip flow egress** or **ip flow ingress** is configured on at least one port. However, you cannot configure **ip flow egress** and **ip flow ingress** on the same port. The latest configuration overwrites the former configuration, affects newly established flows, but does not affect flows that have been established.

Configuration Examples The following example shows how to configure the statistics on the egress IP flow on port 1/1.

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# ip flow ingress
```

Related Commands

Command	Description
ip flow-aggregation cache	Enters IPFIX flow aggregate configuration mode.
snmp-server if-index persist	Ensures the port index remain unchanged when the device is restarted. It is recommanded to enable this function before enabling ipfix.
cache	Configures cache parameters of flow aggregate configuration mode.
export destination (**aggregation cache**)	Exports flow aggregation records to the destination in flow aggregation configuration mode.
mask (**IPv4**)	Specifies the prefix code of source or destination address for prefix aggregation mode.

Platform Description N/A

mask (IPv4)

Use this command to set the prefix mask of source or destination address in flow aggregation configuration mode,. Use the **no** form of this command to restore the default configuration.

mask { [**destination** | **source**] **minimum** *value* }

no mask { [**destination** | **source**] **minimum** }

Parameter Description

Parameter	Description
destination	Sets the prefix mask of destination address.
source	Sets the prefix mask of source address.
minimum	Sets the minimum mask.
value	Sets the number of mask digits in the range 1 to 32.

Defaults The value is 24 by default.

Command Mode Flow aggregation configuration mode

Usage Guide This mode allows you to aggregate flows by IP address. During aggregation, the source or destination address (determined by flow aggregation mode) carries out the AND operation with the mask. The operation result, as the key word, decides which flow the packet belongs to. You can set

the mask as required. If you want the detailed statistics information, choose a mask larger than others; if you want the brief information, choose a mask smaller than others.

Mask configuration is supported in:

Destination address mask aggregation mode (only mask of destination address can be configured)

Destination address mask TOS aggregation mode (only mask of destination address can be configured)

Address mask aggregation mode (masks of source and destination addresses can be configured)

Prefix-port aggregation mode (masks of source and destination addresses can be configured)

Prefix-TOS aggregation mode (masks of source and destination addresses can be configured)

Source prefix aggregation mode (only the mask of source address can be configured)

Source prefix TOS aggregation mode (only the mask of source address can be configured)

Configuration Examples

The following example shows how to configure the mask of source address of **source-prefix** aggregation mode.

```
Ruijie(config)# ip flow-aggregation cache source-prefix
Ruijie(config-flow-cache)# mask source minimum 8
```

The following example shows how to configure the mask of destination address of **destination-prefix** aggregation mode.

```
Ruijie(config)# ip flow-aggregation cache destination-prefix
Ruijie(config-flow-cache)#  mask destination minimum 32
```

Related Commands

Command	Description
ip flow ingress	Collects statistics of ingress flows at an inteface.
ip flow egress	Collects statistics of egress flows at an inteface.
ip flow-cache timeout	Configures the aging time of flow records in cache in main mode.
show ip flow cache	Shows the flow statistics information in the current cache.
show ip flow interface	Shows the IPFIX status.

Platform Description

N/A

show ip flow cache

Use this command to show the overall flow statistics in privileged EXEC mode.

show ip flow cache

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privilege EXEC mode

Usage Guide This command shows the IP flow information and related configuration information in the main cache.

Configuration Examples

```
Ruijie# show ip flow cache
ip flow switching cache, 65536 entries
1 active, 65535 inactive
active flows timeout in 30 minutes
inactive flows timeout in 15 seconds
Protocol    Total Flows       Total packets    Total bytes     Active time
udp-snmp       662                662              48364            0
udp             662                662              48364            0
icmp            623                1289             196076           32
Total:         1285               1951             244440           32
Display entries in main cache :
SrcIf      SrcIPAddress          DstIf      DstIPAddress          Pr      Tos    SrcPort  DstPort  Pkts
ActiveTime
0    192.168.100.3    0    192.168.100.100  1    0    771    0      2    0
...
```

Related Commands

Command	Description
clear ip flow stats	Clears flow statistics information recorded in the system.
show ip flow interface	Shows the IPFIX status at each interface.

Platform Description N/A

show ip flow cache vrf

Use this command to show the statistics of corresponding vrf privileged EXEC mode

show ip flow cache vrf *vrf-name*

Parameter Description

Parameter	Description
vrf-name	Name of the vrf whose statistics are to be shown.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to show statistics of the specified vrf.

Configuration Examples

```
Ruijie# show ip flow cache vrf vrf_name
ip flow switching cache, 0 entries
0 active, 0 inactive
active flows timeout in 30 minutes
inactive flows timeout in 15 seconds
Display entries in aggregation cache :
SrcIf     SrcPrefix            DstIf     DstPrefix
Flows          Pkts             B/Pk         ActiveTime
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip flow cache aggregation

Use this command to show the flow statistics information of flow aggregation mode in privileged EXEC mode.

show ip flow cache aggregation { **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}

Parameter Description

Parameter	Description
destination-prefix	Destination-prefix flow aggregation mode
destination-prefix-tos	Destination address mask TOS flow aggregation mode
prefix	Prefix flow aggregation mode
prefix-port	Prefix-port flow aggregation mode
prefix-tos	Prefix-tos flow aggregation mode
protocol-port	Protocol-port flow aggregation mode
protocol-port-tos	Protocol-port- TOS flow aggregation mode
source-prefix	Sourceprefix flow aggregation mode
source-prefix-tos	Source–prefix-tos flow aggregation mode

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide This command shows therelated configuration information about exporting in each flow aggregation mode.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip flow export

Use this command in privileged EXEC mode to show the flow exporting related configuration information in main mode and other enabled flow aggregation modes,.

show ip flow export [**aggregation** *aggregation-mode*]

Parameter Description

Parameter	Description
destination-prefix	Shows the configurations and statistics of destination-prefix aggregation mode.
destination-prefix-tos	Shows the configurations and statistics of destination-prefix-tos aggregation mode.
prefix	Shows the configurations and statistics of prefix aggregation mode.
prefix-port	Shows the configurations and statistics of prefix-port aggregation mode.
prefix-tos	Shows the configurations and statistics of prefix-tos aggregation mode.
protocol-port	Shows the configurations and statistics of protocol-port aggregation mode.
protocol-port-tos	Shows the configurations and statistics of protocol-port-tos aggregation mode.
source-prefix	Shows the configurations and statistics of source-prefix aggregation mode.
source-prefix-tos	Shows the configurations and statistics of source-prefix-tos aggregation mode.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command shows the flow exporting related configuration information in each flow aggregation mode

Configuration Examples

```
Ruijie# show ip flow export
cache for main metering process:
flow export is disabled
Exporting using default source IP address
Template export information:
Template timeout = 10 minutes
Template refresh rate = 20 packets
total 0 packets metering
total 0 packets dropped for no memory
total 0 flows exported in 0 udp datagrams
0 ipfix message export failed
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip flow interface

Use this command to show the IPFIX configuration information at interfaces in privileged EXEC mode,.

show ip flow interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privilege EXEC mode

Usage Guide This command shows the IP flow information and related configuration information recorded in the cache for each flow aggregation mode.

Configuration

```
Ruijie# show ip flow interface
```

Examples

```
FastEthernet 0/1
ip flow ingress
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

RLOG Commands

rlog enable

Use this command to enable Rlog output.

rlog enable

no rlog enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The Rlog output is disenabled by default.

Command Mode Global configuration mode.

Usage Guide Use this command to output Rlogs onto the Rlog server.

Configuration Examples The following example configures the output rate of Rlogs:

```
Ruijie(config)# rlog enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

rlog export-rate

Use this command to set the rlog export rate.

rlog enable

no rlog enable

Parameter Description

Parameter	Description
number	The rlog export rate

Defaults The Rlog output rate is 1000 by default.

Command Mode Global configuration mode.

Usage Guide The default rlog export rate is comparatively small. You can set the maximum value if the rlog server performance is allowed

Configuration Examples The following example configures the output rate of Rlogs:

```
Ruijie(config)# rlog export-rate 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description The length of a single Rlog is 50 bytes.

rlog mtu

Use this command to configure the maximum log length

rlog mtu *number*

no rlog mtu

Parameter Description

Parameter	Description
number	The maximum log length.

Defaults The maximum length ofa Rlog packet is 1500 by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the maximun length of the Rlog packets:

```
Ruijie(config)# rlog mtu 1500
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

rlog port

Use this command to specify the rlog port number.

rlog port *number*

no rlog port

Parameter Description

Parameter	Description
number	The maximum log length.

Defaults The port number of the Rlog server is 10000 by default.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the port number of the Rlog server:

```
Ruijie(config)# rlog mtu 13000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

rlog server

Use this command to set the IP address for the rlog server and VRF

rlog port *number*

no rlog port

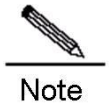
Parameter Description

Parameter	Description
server-ip	IP address for the rlog server.
vrf-name	VRF name.

Defaults The Rlog service is disabled by default.

Command Mode Global configuration mode.

Usage Guide This command is the log switch command. The device will not send the logs to the rlog server without this command configured.
After configuring this command, the logs will be sent in the UDP packet way.



Note that this command only enables the rlog server, and the log output function is not enabled. Use the **ip session log-on** command to output the logs.

Configuration Examples The following example configures the port number of the Rlog server:

```
Ruijie(config)# rlog server 10.1.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

rlog test

Use this command to test the rlog function.
rlog test

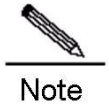
Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode.

Usage Guide Use this command to check the idle buffering and send the test message to the rlog server. Upon receiving the test message, the rlog server can check the server configuration and the network condition based on the corresponding prompting message.



Note that checking the idle buffering will lead to the log loss. To this end, try not to check the idle buffering.

Configuration Examples The following example enables Rlog testing function:

```
Ruijie(config)# rlog test
rlog: 2048 buf remain
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show-rlog

Use this command to show the rlog statistical information.

show rlog

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode.

Usage Guide Use this command to check the idle buffering and send the test message to the rlog server. Upon receiving the test message, the rlog server can check the server configuration and the network condition based on the corresponding prompting message.


Note

Note that checking the idle buffering will lead to the log loss. To this end, try not to check the idle buffering.

Configuration Examples The following example displays the Rlog service statistics information:

```
R Ruijie# show rlog
rlog server is enable
mtu 1200    port 13000    server 10.1.1.1
rlog export-rate 0 rlog queue remain 2048
send log count : 5244 error count : 0 errorno : 0
recv buf: 5244 poll buf err: 0 push buf: 5244
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

HTTP Service

enable service web-server

Use this command to enable the HTTP service function.

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

enable service web-server [**http** | **https** | **all**]

no enable service web-server [**http** | **https**]

Parameter Description

Parameter	Description
http	Enables the HTTP service.
https	Enables the HTTPS service.
all	Enables both the HTTP service and the HTTPS service.

Defaults By default, the HTTP service function is disabled.

Command mode Global configuration mode.

Usage Guide If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

Configuration Examples The following example enables both the HTTP service and the HTTPS service:

```
Ruijie#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Ruijie(config)#enable service web-server
```

Related Commands

Command	Description
show service	Displays the configuration information and status of system service.
show web-server status	Displays the configuration information and status of the web service.

Platform Description N/A

http check-version

Use this command to detect the available upgrade files on the HTTP server.

http check-version

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to detect the available upgrade files. The detected upgrade files version is later than that of local files,

Configuration Examples The following example demonstrates the version of the detected HTTP upgrade file.

```
Ruijie#http check-version
Files need to be updated: web.
app name:web
sn                  version                    filename
-- ------------------- -------------------------
0           1.2.1(82381)        web1.2.1(145680).upd
1           1.2.1(82380)        web1.2.1(145680).upd
2           1.2.1(82379)        web1.2.1(145680).upd
3           1.2.1(82378)        web1.2.1(145680).upd
```

Related Commands

Command	Description
http update	Manually updates designated files.

Platform Description N/A

http update

Use this command to manually update the web file.

http update web [**version** *string*]

Parameter Description

Parameter	Description
string	Version of the Web package to be updated.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to download the available Web package from a remote server to local device.
If the version is specified, then use the update package with specified version to update the Web package; otherwise, use the latest update package to update the Web package.

Configuration Examples The following example demonstrates how to manually download the latest Web package form the designated remote server.

```
Ruijie#http update web
```

Related Commands

Command	Description
http check-vesion	Detects the available update package on the HTTP server.

Platform Description N/A

http update mode

Use this command to configure the HTTP update mode.
http update mode auto-detect
no http update mode

Parameter Description

Parameter	Description
auto-detect	Auto-detect mode

Defaults By default, the auto-detect function is disabled.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTP update mode
Use this command to configure the HTTP working in the auto-detect mode. The device will detect files on the server at detection time. User can check the available Web update files on the Web interface.
Use the **no** form of this command to convert the auto-detect mode into manual mode. The device working in the manual mode cannot update automatically, so the user must configure the update manually.

Configuration Examples The following example enables the Auto-detect mode:

```
Ruijie#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
```

```
Ruijie(config)#http update mode auto-detect
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

http update server

Use this command to configure the IP address and the HTTP port number of the HTTP upgrade server.

http update server { *host-name* | *ip-address* } [**port** *port-number*]

no http update server

Parameter Description

Parameter	Description
host-name	Host name of the HTTP remote upgrade server.
ip-address	IP address of the HTTP remote upgrade server.
port-number	Port number of the HTTP remote upgrade server; value ranges from 1-65535.

Defaults By default, the IP address of the HTTP remote upgrade server is 0.0.0.0 and the port number is 80.

Command mode Global configuration mode.

Usage Guide Use this command to configure the IP address and the HTTP port number of the HTTP upgrade server. When processing the update, the user-configured server address is preferentially used. If the connection fails, the server address in store in the local upgrade record file will be used to establish the connection. When all the above connection fails, the update will be suspended.

At least one IP address of upgrade server is stored in the local upgrade record file, and this IP address cannot be modified.

The HTTP upgrade server address is does not necessarilyneed to be configuredconfigured be ascause the local upgrade record file records available upgrade server addresses.

If the server domain needs to be configured, enable the DNS function on the device and configure the DNS server address.

The server IP address cannot be an IPv6 address.

Configuration Examples The following example configures the IP address and the HTTP port number of the HTTP upgrade server:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#http update server 10.83.132.1 port 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

http update time

Use this command to configure the HTTP auto-detection time

http update time daily *hh*:*mm*

no http update time

Parameter Description

Parameter	Description
hh:*mm*	Specific auto-detection time; (24-hour system); accurate to minute.

Defaults By default, the remote HTTP auto-detection time is random.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTP auto-detection time. The device detects the files available for upgrade on the server at the specified detection time. Use can read these detected file information through Web interface.

Use the **no** form of this command to reset the auto-detection time as random.

Configuration Examples The following example configures the HTTP auto-detection time：

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#http update time daily 23:40
```

Related Commands

Command	Description
http update mode	Configures the HTTP update mode

Platform N/A

Description

http web-file update

Use this command to update the Web package.

http web-file update

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide When the latest installation package is acquired and is stored in local device, user can run this command directly without restarting the device to update the Web package.


Caution To enable the new web package to take effect, log in to the web interface again.

Configuration Examples The following example updates the Web package

```
Ruijie#http web-file update
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip http port

Use this command to configure the HTTP port number.

Use the **no** form of this command to restore the HTTP port number to the default value.

ip http port *port-number*

no ip http port

Parameter Description

Parameter	Description
port-number	Configures the HTTP port number, the value includes 80, 1025-65535.

Defaults The default HTTP port number is 80.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTP port number.

Configuration Examples The following example configures the HTTP port number as 8080:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip http port 8080
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service function.
show web-server status	Displays the configuration information and status of the web service.

Platform Description N/A

ip http secure-port

Use this command to configure the HTTPS port number.

Use the **no** form of this command to restore the HTTPS port number to the default value.

ip http secure-port *port-number*

no ip http secure-port

Parameter Description

Parameter	Description
port-number	Configures the HTTPS port number, the value includes 443, 1025-65535.

Defaults The default HTTP port number is 443.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTPS port number.

Configuration Examples The following example configures the HTTPS port number as 4443:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip http secure-port 4443
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service function.
show web-server status	Displays the configuration information and status of the web service.

Platform Description N/A

show web-server status

Use this command to display the configuration information and status of the web.

show web-server status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration information and status of the web:

```
Ruijie#show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
http(s) use memory block: 768, create task num: 0
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service function.
ip http port	Configures the HTTP port number.
ip http secure-port	Configures the HTTPS port number.

Platform Description N/A

webmaster level

Use this command to configure HTTP authentication information, including the username and password.

webmaster level *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }

no webmaster level *privilege-level* [**username** name]

Parameter Description

Parameter	Description
privilege-level	Configures the user privilege-level.
name	Username.
password	Password.
0 | **7**	Password type; 0 indicates plaintext, 7 indicates ciphertext.
encrypted-password	Password text.

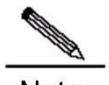
Defaults N/A

Command mode Global configuration mode.

Usage Guide When HTTP is enabled, users can log in to the web interface only after being authenticated. Use this command to configure the username and password for the HTTP authentication information.

Run the command **no webmaster level** *privilege-level I* to delete all the usernames and the password with a designated *privilege-level.*

Run the command **no webmaster level** *privilege-level* **username** *name* to delete the designated username and password.



Note Usernames and passwords come with three permission levels, each of which includes at most 20 usernames and passwords.

Configuration Examples The following example configures HTTP authentication information, including the username and password:

```
Ruijie#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Ruijie(config)#webmaster level 0 username ruijie password admin
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service function.

Platform Description N/A

RADIUS Dynamic Authorization Extension Configuration Commands

clear radius dynamic-authorization-extension statistics

Use this command to clear statistics about RADIUS dynamic authorization extension.

clear radius dynamic-authorization-extension statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

#Clear statistics about RADIUS dynamic authorization extension:

Ruijie# **show radius dynamic-authorization-extension statistics**

Disconnect-Request Received: 50
Incorrect Disconnect-Request Received: 1
Disconnect-Request Dropped for Queue Full: 0
Disconnect-Request Process Timeout: 0
Disconnect-Request Process Success: 49
Disconnect-ACK Sent: 25
Disconnect-ACK Sent Failed: 0
Disconnect-NAK Sent: 24
Disconnect-NAK Sent Failed: 0

Ruijie# **clear radius dynamic-authorization-extension statistics**

Ruijie# **show radius dynamic-authorization-extension statistics**

Disconnect-Request Received: 0
Incorrect Disconnect-Request Received: 0
Disconnect-Request Dropped for Queue Full: 0
Disconnect-Request Process Timeout: 0
Disconnect-Request Process Success: 0
Disconnect-ACK Sent: 0
Disconnect-ACK Sent Failed: 0
Disconnect-NAK Sent: 0
Disconnect-NAK Sent Failed: 0

Related Commands

Command	Description
show radius	Shows statistics about RADIUS

dynamic-authorization-extension statistics	dynamic authorization extension.

Platform Description N/A

radius dynamic-authorization-extension enable

Use this command to enable RADIUS dynamic authorization extension. Use the **no** form of this command to disable this function.

radius dynamic-authorization-extension enable

no radius dynamic-authorization-extension enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RADIUS dynamic authorization extension is disabled by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples #Enable RADIUS dynamic authorization extension.
Ruijie(config)# radius dynamic-authorization-extension enable

Related Commands

Command	Description
show running-config	Checks whether RADIUS dynamic authorization extension is enabled.

Platform Description N/A

radius dynamic-authorization-extension port

Use this command to set a UDP port for receiving packets about RADIUS dynamic authorization extension. Use the **no** form of this command to remove the setting.

radius dynamic-authorization-extension port *num*

no radius dynamic-authorization-extension port

Parameter Description

Parameter	Description
num	Specifies a UDP port for receiving packets about RADIUS dynamic authorization extension. The port number ranges from 1025 to 65535. The default value is 3799.

Defaults The default UDP port number is 3799.

Command mode Global configuration mode

Usage Guide Ensure that the configured UDP port is not being used.

Configuration Examples #Set the UDP port numbered 4000:
Ruijie(config)# **radius dynamic-authorization-extension port** *4000*

Related Commands

Command	Description
show running-config	Shows the UDP port for receiving packets about RADIUS dynamic authorization extension.

Platform Description N/A

show radius dynamic-authorization-extension statistics

Use this command to show statistics about RADIUS dynamic authorization extension.

show radius dynamic-authorization-extension statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to show statistics about RADIUS dynamic authorization extension, including received and sent packets and the processing results about received request packets.

Configuration Examples #Show statistics about RADIUS dynamic authorization extension:
Ruijie# **show radius dynamic-authorization-extension statistics**
Disconnect-Request Received: 50
Incorrect Disconnect-Request Received: 1
Disconnect-Request Dropped for Queue Full: 0
Disconnect-Request Process Timeout: 0
Disconnect-Request Process Success: 49
Disconnect-ACK Sent: 25

Disconnect-ACK Sent Failed:	0
Disconnect-NAK Sent:	24
Disconnect-NAK Sent Failed:	0

Related Commands

Command	Description
clear radius dynamic-authorization-extension statistics	Clears statistics about RADIUS dynamic authorization extension.

Platform Description

N/A

WAN-TA Commands

cong-algorithm

Use this command to specify the congestion algorithm of the WAN-TA policy. Use the **no** form of this command to clear the configuration and restore the default setting.

cong-algorithm { **default** | **high-delay-1** | **high-delay-2** | **high-lost** | **low-bandwidth-delay** }

no cong-algorithm

Parameter Description

Parameter	Description
default	Configures the default congestion algorithm, that is, TCP veno algorithm.
high-delay-1	Configures high-delay-1 algorithm, suitable for high latency network.
high-delay-2	Configures high-delay-2 algorithm, suitable for high latency network.
high-lost	Configures high-lost algorithm, suitable for high drop network.
low-bandwidth-delay	Configures low-bandwidth-delay algorithm, suitable for the network with low bandwidth and latency.

Defaults The self-defined WAN-TA policy adopts the default algorithm. The WAN-TA policy of the system is determined by the system scenario.

Command mode wan-ta policy configuration mode

Usage Guide This command is used to specify the congestion algorithm of the WAN-TA policy. The effect of the WAN-TA policy varies with different algorithms.

Configuration Examples The following example sets the congestion algorithm of the WAN-TA policy to low-bandwidth-delay algorithm.

```
Ruijie(config)#wan-ta policy video
Ruijie(config-wan-ta-policy)#cong-algorithm low-bandwidth-delay
```

Related Commands

Command	Description
wan-ta policy	The **cong-algorithm** *cong-value* parameter of the **wan-ta policy** command shares the same function with the **cong-algorithm** command in wan-ta policy configuration mode, that is, to specify the congestion algorithm of the wan-ta policy.

Platform Description N/A

init-cwnd

Use this command to specify the initial window size of the WAN-TA policy. Use the **no** form of this command to clear the configuration and restore the default setting.
init-cwnd *cwnd-value*
no init-cwnd

Parameter Description

Parameter	Description
cwnd-value	The initial window size ranges from 2 to10 mss. The WAN-TA policy of the system is determined by the system scenario.

Defaults The default initial window size is 10 mss. The WAN-TA policy of the system is determined by the system scenario.

Command mode wan-ta policy configuration mode

Usage Guide This command is used to specify the initial window size of the WAN-TA policy. The larger the window size, the higher initial TCP flow rate.

Configuration Examples The following example sets the initial window size of the WAN-TA policy to 10mss.

```
Ruijie(config)#wan-ta policy video
Ruijie(config-wan-ta-policy)# init-cwnd 10
```

Related Commands

Command	Description
wan-ta policy	The **init-cwnd** ***c****ong-value* parameter of the **wan-ta policy** command shares the same function with the **init-cwnd** command in wan-ta policy configuration mode, that is, to specify the initial window size of the wan-ta policy.

Platform Description N/A

keepalive

Use this command to specify the keepalive packet sending interval of the WAN-TA policy and the

maximum number of keepalive packet retransmission. Use the **no** form of this command to clear the configuration and restore the default settings.

keepalive interval *interval-value* **retry** *retry-count*

no keepalive

Parameter Description

Parameter	Description
interval-value	The keepalive packet sending interval within the range from 2 to 300 minutes.
retry-count	The maximum number of keepalive packet retransmission within the range from 1 to 9. If the retransmission number reaches the upper limit, connection will be reset.

Defaults By default, The keepalive packet sending interval of the self-defined policy and the WAN-TA policy is 120 minutes and the maximum number of keepalive packet retransmission is 9.

Command mode wan-ta policy configuration mode

Usage Guide This command is used to specify the keepalive packet sending interval of the WAN-TA policy and the maximum number of keepalive packet retransmission. The shorter the interval, the more frequent sending keepalive packets

Configuration Examples The following example sets the keepalive packet sending interval to 20 minutes and the maximum number of keepalive packet retransmission to 3.

```
Ruijie(config)#wan-ta policy video
Ruijie(config-wan-ta-policy)#keepalive interval 20 retry 3
```

Related Commands

Command	Description
wan-ta policy	The **keepalive interval** *interval-value* **retry** *retry-count* parameter of the **wan-ta policy** command shares the same function with the **keepalive** command in wan-ta policy configuration mode, that is, to specify the keepalive packet sending interval of the WAN-TA policy and the maximum number of keepalive packet retransmission.

Platform Description N/A

match-port

Use this command to specify the port number that matches the service of WAN-TA implementation. Use the **no** form of this command to clear the configuration.

match-port *port-number* [*port-number…*]

no match-port

Parameter Description

Parameter	Description
port-number	The port number of the video policy implementation ranges from 1 to 65535. A total of 10 ports can be configured.

Defaults By default, the self-defined WAN-TA policy specifies no port. The video policy of the system specifies the number of match port as 554.

Command mode wan-ta-policy configuration mode

Usage Guide This command is used to specify the port number that matches the video service of WAN-TA implementation. By default, the port number that matches the video service of WAN-TA implementation is 554. A total of 10 ports can be configured. If the configured values are repeated or not sorted in order, the system arranges the order automatically. The **no** form of this command is used to clear the configuration, that is, the WAN-TA policy is independent from the service port.

Configuration Examples The following example sets the port number that matches the video service of WAN-TA implementation to 554, 3777.

```
Ruijie(config)#wan-ta policy video
Ruijie(config-wan-ta-policy)#match-port 554 37777
```

The following example sets the video service of WAN-TA implementation independent from the port number.

```
Ruijie(config)#wan-ta policy video
Ruijie(config-wan-ta-policy)#no match-port
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mss

Configures the maximum segment size (MSS) of the WAN-TA policy. Use the **no f**orm of this

command to restore the default setting.

mss *mss- value*

no mss

Parameter Description

Parameter	Description
mss- value	The maximum segment size within the range from 68 to 1460

Defaults By default , the mass value of the WAN-TA policy is 1300.

Command mode wan-ta policy configuration mode

Usage Guide This command is used to specify the MSS value of the WAN-TA policy. The value should be determined by the network environment.

Configuration Examples The following example sets the MSS value of the WAN-TA policy as 1400.

```
Ruijie(config)#wan-ta policy video
Ruijie(config-wan-ta-policy)# mss 1400
```

Related Commands

Command	Description
wan-ta policy	The **mss** *mss-value* parameter of the **wan-ta policy** command shares the same function with the **mss** command in wan-ta policy configuration mode, that is, to specify the MSS value of the WAN-TA policy.

Platform Description N/A

sack

Use this command to enable or disable the sack function of the WAN-TA policy. Use the **no** form of this command to restore default setting.

sack { **enable** | **disable** }

no sack

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the sack function of the WAN-TA policy is enabled.

Command mode wan-ta policy configuration mode

Usage Guide This command is used to enable or disable the sack function of the WAN-TA policy.

Configuration Examples The following example disables the sack function of the WAN-TA policy.

```
Ruijie(config)#wan-ta policy video
uijie(config-wan-ta-policy)#sack disable
```

Related Commands

Command	Description
wan-ta policy	The **sack** parameter of the **wan-ta policy** command shares the same function with the **sack** command in wan-ta policy configuration mode, that is, to enable or disable the sack function of the WAN-TA policy.

Platform Description N/A

show wan-ta policy

Use this command to show configuration information of specified WAN-TA policy.

show wan-ta policy { *policy-name* | **video** }

Parameter Description

Parameter	Description
policy-name	The name of the WAN-TA policy The user-defined policy name cannot be the same as the prefix of the system-defined policy, such as v, vi, vid, vide and video. Otherwise, the system enters the system-defined command with the same prefix automatically.
video	Shows the parameters of video policy implementation.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide This command is used to show configuration information of the specified WAN-TA policy.

Configuration Examples The following example shows the parameters of video policy implementation and the interface that applies the policy.

```
Ruijie#show wan-ta policy video
wan-ta policy: video
    Congestion Control : low-bandwidth-delay
    SACK Support: TRUE
    Initial Congest Window: 10 MSS
    Maxitum Segment Size: 1420
Keepalvie Interval(retry): 120(9)
Match Port: 554
apply on interfaces:
interface name                  list
GigabitEthernet 1/0/0           101
GigabitEthernet 1/0/1           102
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show wan-ta policy session

Use this command to show the TCP session list of the WAN-TA implementation.

show wan-ta policy session [*session_id*]

Parameter Description

Parameter	Description
N/A	Shows summary information on all TCP sessions of the WAN-TA implementation when there is no parameter,
session_id	Shows the detailed information on TCP sessions with correspondent session-id.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Both summary and detailed information on all TCP sessions of the WAN-TA implementation will be shown after enabling the WAN-TA policy.

Configuration Examples The following example shows information on all TCP of the WAN-TA implementation.

```
Ruijie#sh wan-ta  policy session
session_id  pair  flow                          tcp_state              uptime
```

```
6       5       [42.1.1.2:3540->61.147.103.72:21]       TCP_ESTABLISHED             0:40:43
5     6    [61.147.103.72:21->42.1.1.2:3540]            TCP_ESTABLISHED             0:40:43
```

The following example shows detailed statistics on the TCP session whose session ID is 16.

```
Ruijie#show wan-ta policy session 16

[66.2.1.27:1933->192.168.5.120:8000]
(timer notify: 782, handle: 782, signal handle: 29705, while: 5343)
sock state: TCP_ESTABLISHED             ref_cnt: 2
Congestion Control:
   algorithm        : high-delay-1
   icsk_ca_state : open                  icsk_retransmits: 0
   icsk_rto         : 1650 ms            icsk_timeout      : 0 ms
   icsk_backoff   : 0                    icsk_probes_out : 0
   disorder_num   : 5                    cwr_num             : 0
   recovery_num   : 0                    loss_num            : 3
TCP Options:
   is_tstamp        : yes
   is_sack          : yes
   is_wscale        : yes              snd_wscale: 0                  rcv_wscale: 1
Statistics:
   unacked          : 0                  sacked              : 0
   lost             : 0                  retrans             : 0
   in flight        : 0                  fackets             : 0
   total retans   : 3
Times:
   last_data_sent: 5700 ms   last_data_recv: 5710 ms   last_ack_recv: 5030 ms
Keepalive:
   interval         : 600 s              retry               : 3
Metrics:
   usable_wnd       : 64669              bw                  : 0 B/s
   snd_ssthresh   : 2147483647           rcv_ssthresh      : 47744
   snd_cwnd         : 5                  rtt                 : 460 ms
   snd_wnd          : 64669              rttvar              : 290 ms
   reordering       : 3                  rcv_rtt             : 3180 ms
   mss_cache        : 1380               advmss              : 1408
   in_pkt_num       : 150                out_pkt_num       : 157
Queue length:
   recv_queue_len: 0             write_queue_len: 0             ofo_queue_len: 0
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

wan-ta enable

Use this command to enable the WAN-TA implementation. Use the **no** form of this command to disable the WAN-TA implementation.

wan-ta enable

no wan-ta enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the system disables the WAN-TA implementation

Command mode Global configuration mode

Usage Guide Use this command to enable or disable the WAN-TA globally. TCP flows will not be accelerated by enabling the WAN-TA. After configuring the WAN-TA policy, any new flows matching the policy rules will be optimized.

Configuration Examples The following example enables the WAN-TA.

```
Ruijie(config)# wan-ta enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

wan-ta policy

Use this command to enter the configuration of specified WAN-TA policy. If there is no WAN-TA policy with the specified name, the system will create a WAN-TA policy with the specified name. Use the **no** form of this command to clear the configuration. When global WAN-TA and the current policy are applied on the interface, the WAN-TA acceleration policy will be enabled.

wan-ta policy { **video** | *policy-name* } [**cong-algorithm** *cong-value* | **init-cwnd** *cwnd-value* | **sack** { **enable** | **disable** } | **mss** *mss-value* | **keepalive interval** *interval-value* **retry** *retry-count*]]

Parameter Description

Parameter	Description

video	Creates a system-defined policy named video. The system provides parameters suitable for video scenario. The following parameters are optional. If you specify parameters, the system-provided parameters will be replaced. If no parameter is specified, please enter policy configuration mode to specify parameters. System-provided parameters are recommended.
policy-name	Creates a user-defined policy. The system specifies default parameters of the policy. The following parameters are optional. If you specify parameters, the system-provided parameters will be replaced. If no parameter is specified, please enter policy configuration mode to specify parameters. The user-defined policy name cannot be the same as the prefix of the system-defined policy, such as v, vi, vid, vide and video. Otherwise, the system enters the system-defined command with the same prefix automatically.
cong-algorithm *cong-value*	Specifies the congestion algorithm of the WAN-TA policy. The user-defined WAN-TA policy adopts the default algorithm. The WAN-TA policy of the system is determined by the system scenario.
init-cwnd *cwnd-value*	Specifies the initial window size of the WAN-TA policy. By default, the value is 2. The WAN-TA policy is determined by the system scenario.
sack { **enable** | **disable** }	Enables or disables the sack function. By default, the sack function is enabled.
mss *mss-value*	Specifies the MSS of the WAN-TA policy. By default, the value is 1300.
keepalive interval *interval-value* **retry** *retry-count*	Specifies the keepalive packet sending interval of the WAN-TA policy and the maximum number of keepalive packet retransmission. By default, the interval is 120 minutes and the number is 9.

Defaults By default, no WAN-TA policy is applied on the interface.

Command mode Global configuration mode

Usage Guide This command is used to create a specified WAN-TA policy and specify parameters in the following two ways:

1. Add parameters to the command. The [**cong-algorithm** *cong-value* | **init-window** *window-value* | **sack** { **enable** | **disable** } | **mss** *mss-value* | **keepalive interval** *interval-value* **retry** *retry-count*] parameters are optional. You can select one or several parameters. If you don't select any parameter, enter the policy configuration mode to specify the parameters.
2. If there is no optional parameter of the **wan-ta policy** command, you can specify the parameters by running corresponding commands in policy configuration mode.
3. You do not need to specify parameters when creating a system-defined policy. Instead, the system provides parameters. You can specify parameters by the **wan-ta policy** command or by corresponding commands in policy configuration mode when creating a self-defined policy.

Configuration Examples

The following example creates a system-defined video policy.

```
Ruijie(config)#wan-ta policy video
```

The following example creates a user-defined ftp policy.

```
Ruijie(config)#wan-ta policy ftp
Ruijie(config-wan-ta-policy)#init-cwnd 10
Ruijie(config-wan-ta-policy)#cong-algorithm low-bandwidth-delay
```

Related Commands

Command	Description
cong-algorithm	The **cong-algorithm** *cong-value* parameter of the **wan-ta policy** command shares the same function with the **cong-algorithm** command in wan-ta policy configuration mode, that is, to specify the congestion algorithm of the wan-ta policy.
init-cwnd	The **init-cwnd** ***c****ong-value* parameter of the **wan-ta policy** command shares the same function with the **init-cwnd** command in wan-ta policy configuration mode, that is, to specify the initial window size of the wan-ta policy.
mss	The **mss** *mss-value* parameter of the **wan-ta policy** command shares the same function with the **mss** command in wan-ta policy configuration mode, that is, to specify the MSS value of the WAN-TA policy.
sack	The **sack** parameter of the **wan-ta policy** command shares the same function with the **sack** command in wan-ta policy configuration mode, that is, to enable or disable the sack function of the WAN-TA policy.
keepalive	The **keepalive interval** *interval-value* **retry** *retry-count* parameter of the **wan-ta policy** command shares the same function with the **keepalive** command in wan-ta policy configuration mode, that is, to specify the keepalive packet sending interval of the WAN-TA policy and the maximum number of keepalive packet retransmission.

Platform Description

N/A

wan-ta-policy

Use this command to apply the WAN-TA policy on the interface. Use the **no** form of this command to clear the configuration.

wan-ta-policy { *policy-name* | **video** } **list** { *acl-id* | *acl-name* }

no wan-ta-policy { *policy-name* | **video** } **list** { *acl-id* | *acl-name* }

Parameter Description

Parameter	Description
policy-name	Applies the specified policy on the interface. The user-defined policy name cannot be the same as the prefix of the system-defined policy, such as v, vi, vid, vide and video. Otherwise, the system enters the system-defined command with the same prefix automatically.
video	Applies the video policy on the interface.
acl-id	Specifies the ACL number matching the service to be optimized.
acl-name	Specifies the ACL name matching the service to be optimized.

Defaults By default, no WAN-TA policy is applied on the interface.

Command mode Interface configuration mode

Usage Guide This command is used to apply the specified policy on the interface. Any new TCP flows on the interface will be optimized meeting ACL rules of the WAN-TA policy.

Configuration Examples The following example applies the WAN-TA policy named video on the interface gigaethernet 0/0, and optimizes the TCPS flows meeting the ACL rule 101.

```
Ruijie(config)#interface gigaethernet0/0
Ruijie(config-if-GigabitEthernet 0/0)# wan-ta-policy video list 101
```

Related Commands

Command	Description
wan-ta enable	The policy applied on the interface takes effect only when the **wan-ta enable** command is run in global configuration mode.

Platform Description N/A

RADIUS Dynamic Authorization Extension Commands

clear radius dynamic-authorization-extension statistics

Use this command to clear statistics about RADIUS dynamic authorization extension.

clear radius dynamic-authorization-extension statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples #Clear statistics about RADIUS dynamic authorization extension:

```
Ruijie# show radius dynamic-authorization-extension statistics
Disconnect-Request Received:                    50
Incorrect Disconnect-Request Received:          1
Disconnect-Request Dropped for Queue Full:      0
Disconnect-Request Process Timeout:             0
Disconnect-Request Process Success:             49
Disconnect-ACK Sent:                            25
Disconnect-ACK Sent Failed:                     0
Disconnect-NAK Sent:                            24
Disconnect-NAK Sent Failed:                     0

Ruijie# clear radius dynamic-authorization-extension statistics
Ruijie# show radius dynamic-authorization-extension statistics
Disconnect-Request Received:                    0
Incorrect Disconnect-Request Received:          0
Disconnect-Request Dropped for Queue Full:      0
Disconnect-Request Process Timeout:             0
Disconnect-Request Process Success:             0
Disconnect-ACK Sent:                            0
Disconnect-ACK Sent Failed:                     0
Disconnect-NAK Sent:                            0
Disconnect-NAK Sent Failed:                     0
```

Related

Command	Description

Commands

show radius dynamic-authorization-extension statistics	Shows statistics about RADIUS dynamic authorization extension.

Platform Description N/A

radius dynamic-authorization-extension enable

Use this command to enable RADIUS dynamic authorization extension. Use the **no** form of this command to disable this function.

radius dynamic-authorization-extension enable

no radius dynamic-authorization-extension enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RADIUS dynamic authorization extension is disabled by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples #Enable RADIUS dynamic authorization extension.

```
Ruijie(config)# radius dynamic-authorization-extension enable
```

Related Commands

Command	Description
show running-config	Checks whether RADIUS dynamic authorization extension is enabled.

Platform Description N/A

radius dynamic-authorization-extension port

Use this command to set a UDP port for receiving packets about RADIUS dynamic authorization extension. Use the **no** form of this command to remove the setting.

radius dynamic-authorization-extension port *num*

no radius dynamic-authorization-extension port

Parameter Description

Parameter	Description
num	Specifies a UDP port for receiving packets about RADIUS dynamic authorization extension. The port number ranges from 1025 to 65535. The default value is 3799.

Defaults The default UDP port number is 3799.

Command mode Global configuration mode

Usage Guide Ensure that the configured UDP port is not being used.

Configuration Examples #Set the UDP port numbered 4000:

Ruijie(config)# **radius dynamic-authorization-extension port** *4000*

Related Commands

Command	Description
show running-config	Shows the UDP port for receiving packets about RADIUS dynamic authorization extension.

Platform Description N/A

show radius dynamic-authorization-extension statistics

Use this command to show statistics about RADIUS dynamic authorization extension.

show radius dynamic-authorization-extension statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to show statistics about RADIUS dynamic authorization extension, including received and sent packets and the processing results about received request packets.

Configuration #Show statistics about RADIUS dynamic authorization extension:

Examples

```
Ruijie# show radius dynamic-authorization-extension statistics
Disconnect-Request Received:                    50
Incorrect Disconnect-Request Received:          1
Disconnect-Request Dropped for Queue Full:      0
Disconnect-Request Process Timeout:             0
Disconnect-Request Process Success:             49
Disconnect-ACK Sent:                            25
Disconnect-ACK Sent Failed:                     0
Disconnect-NAK Sent:                            24
Disconnect-NAK Sent Failed:                     0
```

Related Commands

Command	Description
clear radius dynamic-authorization-extension statistics	Clears statistics about RADIUS dynamic authorization extension.

Platform Description

N/A

Smart Status Monitoring Commands

smart-monitor schedule

Use this command to configure a smart status monitoring scheduling instance. Use the **no** form of this command to a smart status monitoring scheduling instance.

smart-monitor schedule *schedule-id* **final-seq** *seq-id* **action load** *file-name* **tag-infor [times** *times-number***]**

no smart-monitor schedule *schedule-id*

Parameter Description

Parameter	Description
schedule-id	Indicates the serial number of a smart status monitoring scheduling instance. The value range is from **1** to **8**.
seq-id	Indicates the serial number of an operator. The value range is from **1** to **100**.
file-name	Indicates the name of a to-be-loaded script file. The file name contains 1 to 63 characters.
tag-infor	Executes tagged information in the script. The tagged information contains 1 to 63 characters.
times-number	(Optional) Loads and runs the script labeled by **file-name** when the number of detection times reaches the value of **times-number**. The value range is from **1** to **20**. The default value is **1**.

Defaults By default, no smart status monitoring scheduling instances are configured.

Command Mode Global configuration mode.

Usage Guide The name of the script file to be loaded contains 63 characters at most. Meanwhile, the script file should include related key configurations. The script file is loaded to flash of the device via TFTP in advance.

Configuration Examples The following example creates a smart status monitoring scheduling instance with the ID 1, performs operation starting from Operation Sequence 2, and loads content of the test section in the configuration script one.text if the number of detection times reaches 3.

```
Ruijie#configure
Ruijie(config)# smart-monitor schedule 1 final-seq 2 action load one.text test times 3
Ruijie(config)#
```

Related

Command	Description

Commands		
	smart-monitor seq	Configures the operation sequence for smart status detection.
	show smart-monitor schedule [*id* **[do]]**	Displays information about smart status monitoring scheduling instances.

Platform Description This command is only supported on routers.

smart-monitor seq

Use this command to configure the operation sequence for smart status detection. Use the **no** form of the command to delete an operation sequence for smart status detection.

smart-monitor seq *seq-id* {**seq [not]** *seq-id*} **|** {**status [not]** *status-id*} **[** {**and | or**} {**seq [not]** *seq-id*} **|** {**status [not]** *status-id*} **]**

no smart-monitor seq *seq-id*

Parameter Description

Parameter	Description
seq-id	Specifies the operation sequence ID for smart status detection. The operation sequence ID range is from **1** to **100**.
not	(Optional) Performs the NOT operation via operators.
status-id	Indicates the ID of a smart status monitoring detection event. The value range is from **1** to **64**.
and	Indicates binary operation. The AND operation is performed via the left and right operators.
or	Indicates binary operation. The OR operation is performed via the left and right operators.

Defaults By default, no operation sequences for smart status detection are configured.

Command Mode Global configuration mode

Usage Guide When there are sub-sequences for the operation sequences or monitoring event instances, operation sequences for smart status detection can be configured.

Configuration Examples 1. The following example configures smart status detection for the operation sequence 11 and inverts the result 1.

```
Ruijie#configure
Ruijie(config)# smart-monitor seq 11 seq  not 1
```

2. The following example configures smart status detection for the operation sequence 12, binary operation, status of the smart status monitoring detection event 2 and the operation sequence 1.

```
Ruijie#configure
Ruijie(config)# smart-monitor seq 12 status  2 and seq  1
Ruijie(config)#
```

Related Commands

Command	Description
show smart-monitor seq	Displays the smart status monitoring operation sequence.

Platform Description N/A

smart-monitor status

Use this command to configure smart status monitoring detection events. Use the **no** form of this command to delete smart status monitoring detection events.

smart-monitor status *status-id* { **bfd** *peer-address* {**down** | **up**} [**member-interface** *interface-name*]} | { **interface** *interface-name* { **line** {**down** | **up**} | **lacp** {**selected | unselected**} | **link-quality** { **enable | disable**} *link-quality -value*} } **|** { **track** *track-id* {**up** | **down**} | **{ time-range** *time-range-name* **{active | inactive }**}

no smart-monitor schedule *id*

Parameter Description

Parameter	Description
status-id	Indicates status ID. The event ID range is from **1** to **64**.
bfd *peer-address*	Indicates the peer address of the detected BFD session.
down	Indicates that the detected BFD session is in the down state.
up	Indicates that the detected BFD session is in the up state.
interface-name	Indicates the name of member aggregation port.
interface-name	Indicates the name of the detected interface.
down	Indicates that the line of the detected interface is down.
up	Indicates that the line of the detected interface is up.
selected	LACP of the detected interface is selected.
unselected	LACP of the detected interface is not selected.
enable	This parameter takes effect when the link quality is higher than the configured *link-quality-value*.
disable	This parameter takes effect when the link quality is lower than the configured *link-quality-value*.

link-quality -value	Indicates the link quality value of the detected interface. The value range is from **0** to **100**.
track-Id	Indicates detected track ID. The value range is from **1** to **700**.
time-range-name	Indicates the name of the detected time range.
active	Indicates that the detected time range is in the active state.
inactive	Indicates that the detected time range is in the inactive state.

Defaults No startup file name is defined by default.

Command Mode Global configuration mode

Usage Guide BFD session is used to detect the status of the master aggregation port. But to know the status of member aggregation ports, you need to detect the status of LACP ports.

Configuration Examples 1. The following example configures the UP event of the detected BFD session whose peer address is19.19.19.1 and status ID is 1.

```
Ruijie#configure
Ruijie(config)# smart-monitor status 1 bfd 19.19.19.1 up
Ruijie(config)#
```

2. The following example configures the UP event of the detected interface GigabitEthernet 1/1/0 and status ID is3.

```
Ruijie#configure
Ruijie(config)# smart-monitor status 3 interface gigabitEthernet 1/1/0 line up
Ruijie(config)#
```

3. The following example configures the UP event of the detected Track whose number is 1 and status ID is 4.

```
Ruijie#configure
Ruijie(config)# smart-monitor status 4 track 1 up
Ruijie(config)#
```

4. The following example configures the UP event of the detected BFD session whose peer end is the member interface GigabitEthernet 0/0 with the address of 19.19.19.1, and the status ID is 5.

```
Ruijie#configure
Ruijie(config)# smart-monitor status 5 bfd 19.19.19.1 up member-interface GigabitEthernet 0/0
Ruijie(config)#
```

Related Commands

Command	Description
smart-monitor seq	Configures the operation sequence for smart status detection.
show smart-monitor status [*status-id***]**	Displays information about smart status monitoring detection events.

Platform Description N/A

smart-monitor tick

Use this command to configure the scheduling heartbeat period for smart status monitoring. Use the no form of the command to restore the default setting.

smart-monitor tick *seconds*

no smart-monitor tick

Parameter Description

Parameter	Description
seconds	Sets the scheduling heartbeat period for smart status monitoring in seconds. The value range is from **1** to **60**.

Defaults By default, the scheduling heartbeat period for smart monitoring is 5 seconds.

Command Mode Global configuration mode

Usage Guide The configured tick value takes effect on all scheduling instances.

Configuration Examples The following example configures the scheduling heartbeat period for smart status monitoring.

```
Ruijie#configure
Ruijie(config)#smart-monitor tick 10
Ruijie(config)#
```

Related Commands

Command	Description
smart-monitor schedule	Configures a smart status monitoring scheduling instance.

Platform Description This command is only supported on routers.

show smart-monitor schedule

Use this command to display information about smart status monitoring scheduling instances.

show smart-monitor schedule *[schedule-id* [**do**]*]*

Parameter Description

Parameter	Description
schedule-id	The ID of smart status monitoring scheduling instance. The range is from 1 to 8.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples 1. Run the **show smart-monitor schedule** command to display information about all operation scheduling instances.

```
Ruijie#show smart-monitor schedule
smart-monitor schedule 1 final-seq 2 action load one.text test1 times 3
smart-monitor schedule 2 final-seq 1 action load one.text test2 times 1
smart-monitor schedule 3 final-seq 1 action load one.text test3 times 2
```

2. Run the **show smart-monitor schedule 2** command to display information about a specified operation scheduling instance.

```
Ruijie#show smart-monitor schedule 2
smart-monitor schedule 2 final-seq 1 action load one.text test2 times 1
```

3. Run the **show smart-monitor schedule 2 do** command to display information about a specified operation scheduling instance.

```
Ruijie#show smart-monitor schedule 2 do
smart-monitor schedule 2 final-seq 1 action load one.text test2 times 1
```

Field Interpretation

Command	Description
do	Displays information about smart status monitoring scheduling instances while loading script.

Related Commands

Command	Description
smart-monitor schedule	Configures a smart status monitoring scheduling instance.

Platform This command is only supported on routers.

Description

show smart-monitor seq

Use this command to display the smart status monitoring operation sequence.

show smart-monitor seq [*seq-id*]

Parameter Description

Parameter	Description
seq-id	Specifies the sequence ID. The range is from 1 to 100.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples 1. Run the **show smart-monitor seq** command to display all smart status monitoring operation sequences.

```
Ruijie#show smart-monitor seq
smart-monitor seq 5 : final-status True
smart-monitor seq 5    status 2
smart-monitor seq 6 : final-status False
smart-monitor seq 6 not status 2
smart-monitor seq 10 : final-status Fail
smart-monitor seq 10    seq 1
smart-monitor seq 13 : final-status True
smart-monitor seq 13    seq 5
smart-monitor seq 16 : final-status False
smart-monitor seq 16 seq    5 and seq    6
```

2. Run the command to display the specified smart status monitoring operation sequence.

```
Ruijie#show smart-monitor seq 16
smart-monitor seq 16 : final-status False
smart-monitor seq 16 seq    5 and seq    6
Ruijie(config)#
```

Field Interpretation

Field	Interpretation
final-status	Display the final status of smart status monitoring operation sequences: **True**, **False**, or **Fail**.

Related

Command	Description

Commands		
	smart-monitor seq	Configures the operation sequence for smart status detection.
	show smart-monitor status	Displays information about smart status monitoring detection events.

Platform Description N/A

show smart-monitor status

Use this command to display information about smart status monitoring detection events.

show smart-monitor status [*status-id*]

Parameter Description	Parameter	Description
	status-id	(Optional) Specifies the sequence ID of smart status monitoring detection events.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples 1. Run the **show smart-monitor status** command to display information about all smart status monitoring detection events.

```
Ruijie#show smart-monitor status
Smart-monitor status 1 : final-status Fail
smart-monitor status 1 bfd 19.19.19.1 up
Smart-monitor status 3 : final-status Fail
smart-monitor status 3 track 1 up
Smart-monitor status 4 : final-status False
smart-monitor status 4 interface GigabitEthernet 1/1/0 line down
```

2. Run the **show smart-monitor status** 3 command to display information about the specified smart status monitoring detection events.

```
Ruijie#show smart-monitor status 3
Smart-monitor status 3 : final-status True
smart-monitor status 3 track 1 up
```

Field Interpretation

Command	Description
final-status	The result of a smart status monitoring detection event may be **True**, **False**, or **Fail**. **True** indicates a match, **False** indicates a mismatch, and **Fail** indicates that the configuration is incorrect and does not

	meet the detection target.

Related Commands

Command	Description
smart-monitor status	Configures smart status monitoring detection events.

Platform Description This command is only supported on routers.

DNS Parser Commands

dns-parser enable

Use this command to enable DNS forward proxy on an interface. Use the **no** form of this command to restore the default setting on an interface.

dns-parser enable

no dns-parser enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, DNS forward proxy is disabled.

Command Mode Interface configuration mode.

Usage Guide DNS parser examines DNS response packets sent from the interface and add the IP address into the user group associated with the URL group. This command is usually configured on the intranet interfaces.

Configuration Examples The following example enables DNS forward proxy on the interface GigabitEthernet 1/1/1.

```
Ruijie(config)#interface GigabitEthernet 1/1/1
Ruijie(config-if-GigabitEthernet 1/1/1)#dns-parser enable
Ruijie(config-if-GigabitEthernet 1/1/1)#exit
Ruijie(config)#
```

Related Commands

Command	Description
url-group	Creates a URL group.

Platform Description N/A

URL-Class Commands

url-class

Use this command to create a URL class. Use the **no** form of this command to delete a URL class.

url-class *class-name*

no url-class *class-name*

Parameter Description

Parameter	Description
class-name	Name of a URL class containing up to 32bytes.

Defaults

By default, there are nine types of URL class, which cannot be deleted:

Education

Game

Financial

Map-Navigation

Live-Meeting

IM

Web page-Email-General Appliacations

Download-Update- Demand

Other

Command Mode

Global configuration mode.

Usage Guide

Enable url-lib before creating a url class.

Configuration Examples

The following example creates a URL class.

```
Ruijie(config)# url-class test_class
Ruijie(config-url-class)#url www.ruijie.com.cn
Ruijie(config-url-class)#url *.edu.cn
Ruijie(config-url-class)#exit
Ruijie(config)#
```

Related Commands

Command	Description
url	Adds a URL into a URL class.
description	Adds description for a URL class.

Platform Description

N/A

url

Use this command to add a URL into a URL class. Use the **no** form of this command to remove a URL from a URL class.

url *string*

no url *string*

Parameter Description

Parameter	Description
string	A URL string, such as www.ruijienetworks.com.

Defaults N/A

Command Mode URL-Class configuration mode.

Usage Guide The wildcard "*" is supported. It stands for one or more complete domain names and should be put in either the first or the last place of a URL string, like *.edu.cn and www.ruijie.*.

During search, manually-configured URLs take precedence over URLs in the URL library.

Configuration Examples The following example configures a URL class and then adds two URLs into the class.

```
Ruijie(config)# url-class test_class
Ruijie(config-url-class)#url www.ruijie.com.cn
Ruijie(config-url-class)#url *.edu.cn
Ruijie(config-url-class)#exit
Ruijie(config)#
```

Related Commands

Command	Description
url-class	Creates a URL class.

Platform Description N/A

description

Use this command to add description for a URL class. Use the **no** form of this command to delete the description of a URL class.

description *string*

no description

Parameter Description

Parameter	Description
string	Description of a URL class.

Defaults N/A

Command Mode URL-Class configuration mode.

Usage Guide N/A

Configuration Examples The following example configures description for a URL class.

```
Ruijie(config)# url-class test_class
Ruijie(config-url-class)#description custom test
Ruijie(config-url-class)#exit
Ruijie(config)#
```

Related Commands

Command	Description
url-class	Creates a URL class.

Platform Description N/A

URL-Group Commands

url-group

Use this command to create a URL group. Use the **no** form of this command to delete a URL group.

url-group *num*

no url-group *num*

Parameter Description

Parameter	Description
num	Group ID ranging from 1 to 32.

Defaults By default, no URL group is configured.

Command Mode Global configuration mode.

Usage Guide Enable url-lib before creating a URL group.

Configuration Examples The following example creates a URL group.

```
Ruijie(config)# url-group 3
Ruijie(config-url-group)#class cnki
Ruijie(config-url-group)#relate user-group cnki
Ruijie(config-url-group)#exit
Ruijie(config)#
```

Related Commands

Command	Description
class	Associates a URL group with a URL class.
relate user-group	Associates a URL group with a user group.
description	Adds description for a URL group.

Platform Description N/A

class

Use this command to associate a URL group with a URL class. Use the **no** form of this command to remove the association.

class *class-name*

no class

Parameter Description

Parameter	Description
class-name	Class name.

Defaults By default, there are no URL groups.

Command Mode URL-Group configuration mode.

Usage Guide One URL group can be associated to only one URL class.

Configuration Examples The following example associates url-group 3 with the url-class named “cnki”.

```
Ruijie(config)# url-group 3
Ruijie(config-url-group)#class cnki
Ruijie(config-url-group)#exit
Ruijie(config)#
```

Related Commands

Command	Description
url-group	Creates a URL group.

Platform Description N/A

relate user-group

Use this command to associate a URL group with a user group. Use the **no** form of this command to remove the association.

relate user-group *group_name*

no relate user-group

Parameter Description

Parameter	Description
group_name	Name of a user group.

Defaults By default, no URL groups are configured.

Command Mode URL-Group configuration mode.

Usage Guide Only already-existing user groups can be related.

One URL group can be related with only one user group.

Configuration Examples The following example associates url-group3 with a URL group named “cnki”.

```
Ruijie(config)# url-group 3
Ruijie(config-url-group)#relate user-group cnki
Ruijie(config-url-group)#exit
```

```
Ruijie(config)#
```

Related Commands	Command	Description
	url-group	Creates a URL group.

Platform Description N/A

description

Use this command to add description for a URL group. Use the **no** form of this command to delete the description of a URL group.

description *string*

no description

Parameter Description	Parameter	Description
	string	Description of a URL group.

Defaults By default, no URL groups are configured.

Command Mode URL-Group configuration mode.

Usage Guide N/A

Configuration Examples The following example configures description for URL-group 3.

```
Ruijie(config)# url-group 3
Ruijie(config-url-group)#description education association group
Ruijie(config-url-group)#exit
Ruijie(config)#
```

Related Commands	Command	Description
	url-group	Creates a URL group.

Platform Description N/A

url-group ttl

Use this command to configure TTL of IP addresses of the user group that is associated with a URL group. Use the **no** form of this command to restore the default setting.

url-group ttl *minutes*

no url-group ttl *minutes*

Parameter Description

Parameter	Description
minutes	Time to live of IP addresses. The unit is minute and the range is from 1 to 360.

Defaults By default, no TTL of IP addresses is configured.

Command Mode Global configuration mode.

Usage Guide After this command is configured, if not refreshed within the TTL, all IP addresses of the user group associated with a URL group are removed, to ensure availability of stored DNS answer IP addresses and a proper size of the user group.

Configuration Examples The following example sets the TTL to 30minutes.

```
Ruijie(config)# url-group ttl 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

URL-LIB Commands

url-lib enable

Use this command to enable the URL library. Use the **no** form of this command to restore the default setting.

url-lib enable

no url-lib enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the URL library is disabled.

Command Mode Global configuration mode.

Usage Guide Before enabling the URL library, ensure there already exists the library file, flash:/urlib/lib.dat. You can download the library file via such ways as tftp or ftp:

copy tftp://101.101.101.155/lib.dat

flash:/urlib/lib.dat

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

url-lib reload

Use this command to reload the URL library.

url-lib reload

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode	Global configuration mode.
Usage Guide	Before enabling the URL library, ensure there already exists the library file, flash:/urlib/lib.dat. You can download the library file via such ways as tftp or ftp: copy tftp://101.101.101.155/lib.dat flash:/urlib/lib.dat
Configuration Examples	N/A

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

Routing Protocol Commands

Protocol-independent Commands

accept-lifetime

Use this command to specify the lifetime of an encryption key in its receiving direction in encryption key configuration mode. 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 of the encryption key. 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—date 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 lifetime of the encryption key. It must be later than the start time.
duration *seconds*	Duration of the encryption key from the start time. The value ranges from 1 to 2147483646.

Defaults Infinite

Command Mode Encryption key configuration mode

Usage Guide Use this command to specify the lifetime of an encryption key in its receiving direction.

Configuration Examples The following example sets the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011.

```
Ruijie(config)# key chain ripkeys
Ruijie(config)# key 1
Ruijie(config)# accept-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip community-list

Use this command to define a community list and control access to it. Use the **no** form of this command to delete the setting.

ip community-list { { **standard** | **expanded** } *community-list-name* | *community-list-number* } { **permit** | **deny**} [*community-number.*.]

no ip community-list { { **standard** | **expanded** } *community-list-name* | *community-list-number* }

Parameter Description

Parameter	Description
standard	Standard community list
expanded	Expanded community list
community-list-name	Name of the community list, which is a string of at most 80 characters.
community-list-number	Number of the community list:The number of the standard community list ranges from 1 to 99. The number of the expanded community list ranges from 100 to 99.
permit	Permits access to the community list.
deny	Denies access to the community list.
community-number	COMMUNITY attribute value in the format of AA:NN (AS number:2-byte numerical) or a value in the range from 0 to 4294967295. It may also be one of the following pre-defined value: *internet*: indicates the Internet community. All paths belong to this community. *local-as*: indicates that this path will be advertised within the AS. After AS confederation is configured, this path will not be advertised to other ASs or sub-ASs. *no-advertise*: indicates that this path will not be advertised to any BGP peers. *no-export*: indicates that this path will not be advertised to any EBGP peers. This number is a string in the range from 1 to 255 characters. Note: Currently, each community list supports at most 32 community attribute values.

Defaults No community list is defined by default.

Command Mode Global configuration mode

Usage Guide Use this command to define the community list for the BGP.

Configuration Examples

```
Ruijie(config)# ip community-list standard test deny 100:20 200:20
Ruijie(config)# ip community-list standard test2 permit internet
```

Related Commands

Command	Description
match community	Matches the community list.
set comm-list delete	Deletes the COMMUNITY attribute value of a BGP path according to the community list.
show ip community-list	Shows the community list information.
show ip bgp community-list	Shows information about a BGP route that matches the community list.

Platform Description N/A

ip default-network

Use this command to configure the default network globally. Use the **no** form of this command to delete the setting.

ip default-network *network*

no ip default-network *network*

Parameter Description

Parameter	Description
network	Number of the default network

Defaults 0.0.0.0/0

Command Mode Global configuration mode

Usage Guide

The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not a directly connected network.

The default network always starts with an asterisk (*), indicating that it is the candidate of the default route. If connected routes and the routes without next hops exist in the default network, the default route must be a static route.

Configuration Examples

The following example sets 192.168.100.0 as the default network. Since the static route is configured for the network, the device automatically generates a default route.

```
Ruijie(config)# ip route 192.168.100.0 255.255.255.0 serial  0/1
Ruijie(config)# ip default-network 192.168.100.0
```

The following example sets 200.200.200.0 as the default network. This route becomes the default one only when it is available in the routing table.

```
Ruijie(config)# ip default-network 200.200.200.0
```

Related Commands	Command	Description
	show ip route	Shows the IP routing table.

Platform Description N/A

ip fast-reroute route-map

Use this command to configure the static fast reroute. Use the **no** form of this command to disable a static fast reroute.

ip fast-reroute [**vrf** *vrf-name*] **static route-map** *route-map-name*

no ip fast-reroute [**vrf** *vrf-name*] **route-map**

Parameter Description

Parameter	Description
vrf-name	VRF name
route-map-name	The route map for the static route fast reroute.
static	Generates a backup route for the specified static route.

Defaults Disabled

Command mode Global configuration mode

Usage Guide The fast reroute function assigns both the primary and backup routes. When the primary route failes, the router perform a failover to the backup route automatically to shorten the duration of service suspension.

The primary next hop can be enabled with Bidirectional Fowarding Detection (BFD) for better performance of the fast reroute. The primary egress interface can be configured with parameter **carrier-delay** *0* to in interface configuration mode to achieve the fastest failover shorten the duration to shorten the duration of service suspension.

If the primary next hop of a static fast reroute fails and the standby next hop is available, the standby next hop serves as the primary next hop.

Configuration Examples The following example sets the backup next hop to 192.168.1.2 on interface 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 Commands	Command	Description
	fast-reroute	Configures an OSPF fast reroute.

Platform Description N/A

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 delete a prefix list or an entry in the prefix list.

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 from 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, and that of each subsequent one without a sequence number is a number that is a multiple of the first value 5 and larger than the previous sequence number.
deny	Denies the access to the matching result.
permit	Permits the access to the matching result.
ip-prefix	Network address and mask. The network address can be any valid IP address and the mask length is in the range from 0 to 32.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: ge indicates the operation of "greater than" or "equal to".
maximum-prefix-length	(Optional) Maximum length of the prefix (the ending length) Note: le indicates the operation of "less than" or "equal to".

Defaults No prefix list is created by default.

Command Mode Global configuration mode

Usage Guide

Use this command to configure the prefix list, which uses the keyword permit or deny to determine the action in the 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 that the range is from the minimum-prefix-length to 32. **le** indicates that the range is from the mask length of the IP prefix to the maximum-prefix-length. **ge** and **le** indicate that the range is from the minimum-prefix-length to the maximum-prefix-length. That is, the mask length of IP prefix is less than the minimum-prefix-length, and the minimum-prefix-length is less than the maximum-prefix-length which is less than or equal to 32.

Configuration Examples

The following example filters the RIP routes the OSPF redistributes based on the destination IP address. The filter rules are defined in the associated IP prefix list. For example, redistribute the routes whose destination IP address is within 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip prefix-list description

Use this command to add descriptions for a prefix list. Use the **no** form of this command to delete the descriptions.

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

Defaults

No description is added for a prefix list by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example adds a description for an IP prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description Deny routes from Net-A
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip prefix-list sequence-number

Use this command to enable the sorting function for a prefix list. Use the **no** form of this command to disable the function.

ip prefix-list sequence-number

Parameter Description

Parameter	Description
N/A	N/A

Defaults No sorting function is enabled for the prefix list by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example shows the prefix list for which the sort function is enabled:

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list sequence-number
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip route

Use this command to configure a static route. Use the no form of this command to delete the configured route.

ip route [**vrf** *vrf_name*] *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent** | **track** *object-number*] [**weight** *number*] [**disable** | **enable**]

Parameter Description

Parameter	Description
vrf-name	Name of the VRF, which can be a single protocol IPv4 VRF or the multi-protocol VRF of a configured IPv4 address family.
network	Network address of the target network
net-mask	Mask of the target network
ip-address	Next hop IP address of the static route
interface	(Optional) Next hop egress of the static route
distance	(Optional) Management distance of the static route
tag	(Optional) Tag of the static route

permanent	(Optional) Permanent route ID
track *object-number*	(Optional) Object ID for tracking specified in the object-number command that associates with the track object
weight *number*	(Optional) Weight number of the static route
disable/enable	(Optional) Disablement or enablement ID of the static route

Defaults N/A

Command Mode Global configuration mode.

Usage Guide

The default management distance of the static route is 1. Setting the management distance allows the learned dynamic route to overwrite the static route. The static route is used only when no dynamic route is learned. Setting the management distance of the static route enables the route backup, and the static route is also called a floating route in this case. For example, the management distance of the OSPF route protocol is 110. You can set the management distance of the static route 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. If the specified VRF is a multi-protocol VRF, the static route can be configured only for the multi-protocol VRF that is configured for the IPv4 address family. When the IPv4 address family of the VRF is deleted, the IPv4 static route of the VRF will also be deleted.

The default weight of the static route is 1. To view the static route of non-default weights, execute the show ip route weight command. The weight parameter is used to enable the WCMP. When there are load-balanced routes to a destination address, the device assigns data flows by their weights. The higher the weight of a route is, the more data packets the route carries. The WCMP limit is generally 32 for routers. However, the WCMP limit varies depending on switch models because their chipsets support different weights. When the sum of the weights of load-balanced routes exceeds this weight limit, the excessive routes 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 uses the permanent route until the 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 target networks are directly connected to the Fastethernet 0/0 interface. So it sends an ARP request to every target host, which occupies many CPU and memory resources. It is not recommended that the static route be set to directly pointing to an Ethernet interface.

You can specify association between the static route and the specified track object. If the association of the static route with the specified track object is configured, and if the track object is advertised to be inactive, the static route takes no effect. If the track object is advertised to be active, whether the static route takes effect depends on the status of other parties. The association with the specified track object may apply to the situation where the status of a third party that the track object relates to is used to decide whether the static route takes effect. The association with the specified track object and the permanent function are mutually exclusive.

Configuration The following example adds a static route to the target network 172.16.100.0/24 whose next hop is

Examples 192.168.12.1 and management distance is 15.

```
ip route 172.16.100.0 255.255.255.0 192.168.12.1 115
```

If the static route has no specified interface, data flows may be sent through other interfaces in the case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the target network 172.16.100.0/24.

```
Ruijie(config)# ip route 172.16.100.0 255.255.255.0 fastethernet 0/0
192.168.12.1
```

Related Commands

Command	Description
show ip route	Shows the IP routing table.

Platform Description N/A

ip routing

Use this command to enable the IP routing function for the RGOS in global configuration mode. Use the **no** form of this command to disable the function.

ip routing

no ip routing

Parameter Description

Parameter	Description
N/A	N/A

Defaults Enabled

Command Mode Global configuration mode.

Usage Guide This function can be disabled when the device is just used as a bridge or a VoIP gateway.

Configuration Examples The following example disables the IP routing function.

```
Ruijie(config)# no ip routing
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip static route-limit

Use this command to set the upper threshold of the number of the static routes. Use the **no** form of this command to restore the setting to the default value.

ip static route-limit number

no ip static route-limit number

Parameter Description

Parameter	Description
number	Upper threshold of the number of the static routes, which is in the range from 1 to 10000.

Defaults 1024

Command Mode Global configuration mode.

Usage Guide The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes by executing the **show running-config** command.

Configuration Examples The following example sets the upper threshold of the number of the static routes to 900 and then restores the setting to the default value.

```
Ruijie(config)# ip static route-limit 900
Ruijie(config)# no ip static route-limit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 prefix-list

Use this command to create an IPv6 prefix list or add an entry to 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 in the range from 1 to

	2147483647. If the sequence number is not specified in this command, the system allocates a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one without a sequence number is a number that is a multiple of the first value 5 and larger than the previous sequence number.
deny	Denies the access to the matching result.
permit	Permits the access to the matching result.
ipv6-prefix	Network address and its mask. The network address can be any valid IP address. The mask length is in the range from 0 to 128.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: ge indicates the operation of "greater than" or "equal to".
maximum-prefix- length	(Optional) Maximum length of the prefix (the ending length) Note: le indicates the operation of "less than" or "equal to".

Defaults No prefix list is created by default.

Command Mode Global configuration mode

Usage Guide

Use this command to configure an IPv6 prefix list, which uses the keyword permit or deny to determine the action in the 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 that the range is from the minimum-prefix-length to 128. **le** indicates that the range is from the mask length of the ipv6-prefix to the maximum-prefix-length. **ge** and le indicate that the range is from the minimum-prefix-length to the maximum-prefix-length. That is, the mask length of the Ipv6-prefix is less than the minimum-prefix-length, and the minimum-prefix-length is less than the maximum-prefix-length which is less than or equal to 128.

Configuration Examples

The following example filters the RIP routes the OSPF process 1 redistributes based on the destination IP address. The filter rules are defined in the associated IPv6 prefix list. For example, redistribute the routes whose destination IP address is within the range 2222::/64.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre permit 2222::/64
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# redistribute ospf 1
Ruijie(config-router)# distribute-list prefix pre out
Ruijie(config-router)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 prefix-list description

Use this command to add descriptions for an IPv6 prefix list. Use the no form of this command to delete the descriptions.

ipv6 prefix-list *prefix-list-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

Defaults No description is added for an IPv6 prefix list by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example adds a description for an IPv6 prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 disable the function.

ipv6 prefix-list sequence-number

Parameter Description

Parameter	Description
N/A	N/A

Defaults No sorting function is enabled for the prefix list by default.

Command Mode Global configuration mode

Usage Guide None

Configuration Examples

The following example enables the sorting function for an IPv6 prefix list:

```
Ruijie# configure terminal
Ruijie(config)# ipv6 prefix-list sequence-number
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 route

Use this command to configure an ipv6 static route in global configuration mode. Use the **no** form of this command to delete the configured route.

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*] [**weight** *number*]

Parameter Description

Parameter	Description
vrf-name	Name of the VRF that the route belongs to, which must be a multi-protocol VRF of a configured IPv6 address family.
ipv6-prefix	IPv6 prefix, which must use the address form of RFC4291.
prefix-length	Length of the IPv6 prefix, which must follow the slash (/).
ipv6-address	Next hop IP address of the static route
interface	(Optional) Next hop egress of the static route
vrf-name1	Name of the VRF that the next hop belongs to, which must be a multi-protocol VRF of a configured IPv6 address family.
distance	(Optional) Management distance of the static route
number	(Optional) Weight value of the static route, which is specified when configuring the equivalent paths and is in range from 1 to 128. The sum of the weight of all equivalent paths of one route cannot exceed the number of the configurable maximum equivalent paths of the route. The weight ratio between the equivalent paths of the same route indicates the flow rate between these paths.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

When the multi-protocol VRF deletes the IPv6 address family, the VRF that the route belongs to is deleted or the VRF that the next hop belongs to is configured to be the IPv6 static route of the VRF.
If the VRF that the IPv6 static route interface belongs to is not the same as the configured next hop VRF, then this IPv6 static route takes no effect.
The default management distance of the static route is 1. Setting the management distance allows

the learned dynamic route to overwrite the static route. The static route is used only when no dynamic route is learned. Setting the management distance of the static route enables the route backup, and the static route is also called a floating route in this case. For example, the management distance of the OSPF route protocol is 110. You can set its management distance to 125. Then the data can switch over the static route when the route running OSPF fails.

Configuration Examples

The following example adds a static route to the target network 2001::/64 whose next hop is 2002::2 and management distance is 115.

```
ipv6 route 2001::/64 2002::2 115
```

If the static route has no specified interface, data flows may be sent through other interfaces in the case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the target network of 2001::/64.

```
ipv6 route 2001::/64 fastethernet 0/0 2002::2
```

Related Commands

Command	Description
show ipv6 route	Shows the IPv6 routing table.

Platform Description

This command is not supported on a layer-2 device.

ipv6 static route-limit

Use this command to set the upper threshold of the number of the static routes. Use the **no** form of this command to restore the setting to the default value.

ipv6 static route-limit *number*

no ipv6 static route-limit

Parameter Description

Parameter	Description
number	Upper threshold of the number of the static routes, which is in the range from 1 to 10000.

Defaults

1000

Command Mode

Global configuration mode

Usage Guide

The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes by executing the **show running-config** command.

Configuration Examples

The following example sets the upper threshold of the number 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	Shows the IPv6 routing table.

Platform Description N/A

ipv6 unicast-routing

Use this command to enable the IPv6 routing function for the RGOS in global configuration mode. Use the **no** form of this command to disable the function.

ipv6 unicast-routing

no ipv6 unicast-routing

Parameter Description

Parameter	Description
N/A	N/A

Defaults Enabled

Command Mode Global configuration mode

Usage Guide This function can be disabled when the device is just used as a bridge or a VoIP gateway.

Configuration Examples The example disables the IPv6 routing function for the RGOS

```
Ruijie# no ipv6 unicast-routing
```

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.
show ipv6 route	Shows the IPv6 routing table.

Platform Description N/A

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 a specified key.

key *key-id*

no key *key-id*

Parameter Description

Parameter	Description
key-id	Key ID, ranging from 0 to 2147483647.

Defaults No encryption key is defined by default.

Command Mode Encryption key chain configuration mode

Usage Guide Use this command to define an encryption key.

Configuration Examples The following example configures the encryption key chain ripkeys and key 1 and enters the configuration mode of key 1.

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

key chain

Use this command to define a key chain and enter the key chain configuration mode in global configuration mode. Use the **no** form of this command to delete the definition.

key chain *key-chain-name*

no key chain *key-chain-name*

Parameter Description

Parameter	Description
key-chain-name	Key chain name

Defaults No key chain is defined by default.

Command Mode Global configuration mode

Usage Guide You must configure at least one key to enable a key chain to take effect.

Configuration Examples The following example configures the key chain ripkeys and enters the key chain configuration mode.

```
Ruijie(config)# key chain ripkeys
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

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	Shows a key in plain texts.
	7	Shows a key in encrypted texts.
	text	Indicates the authentication strings.

Defaults No key string is configured by default.

Command Mode Encryption key chain configuration mode

Usage Guide Use this command to specify a key string.

Configuration Examples The following example configures the key chain ripkeys, key 1, and key string abc:

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)#key-string abc
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

match as-path

Use this command to redistribute an AS_PATH attribute route permitted in the access list. Use the **no** form of this command to delete the setting.

match as-path *as-path-acl-list-num* [*as-path-acl-list-num*…..]

no match as-path [*as-path-acl-list-num*……]

Parameter Description

Parameter	Description
as-path-acl-list-num	ACL number in the range from 1 to 500.

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide This command can be followed by multiple access list numbers.
One or more match or set commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

```
Ruijie(config)# route-map ROUTEMAP2IBGP
Ruijie(config-route-map)# match as-path 20 30
```

Related Commands

Command	Description
match community	Matches the route community.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.

Platform Description N/A

match community

Use this command to redistribute a COMMUNITY attribute route permitted in the access list. Use the no form of this command to delete 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 community list: Number of the standard community list in the range from 1 to 99. Number of the expanded community list in the range from 100 to 199
communitys-list-name	Name of the community list, which should not exceed 80 characters.
exact-match	Exact match list

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command can be followed by multiple community list numbers or names, but the total of the community list numbers and names should not be greater than 6.

Each keyword exact-match applies only to the previous list.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

```
Ruijie(config)# ip community-list 1 permit 100:2 100:30
Ruijie(config)# route-map set_lopref
Ruijie(config-route-map)# match community 1 exact-match
Ruijie(config-route-map)# set  local-preference 20
```

Related Commands

Command	Description
ip community-list	Defines the community list.
match as-path	Matches the AS_PATH attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute value for the redistributed route.
set comm-list delete	Deletes the matched COMMUNITY attribute value.
set community	Sets the attribute value for the specified community.
set metric	Sets the metric value for the redistributed route.

Platform Description N/A

match interface

Use this command to set the next hop interface as the specified interface. Use the no form of this command to delete 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

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command can be followed by multiple interfaces.

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The route-map can be configured very flexibly and applies to the route redistribution and the policy-based routing configuration. No matter how the route-map is used, the configuration principle is the same, except that different command sets are used. Even if the route-map is used for the route redistribution, different routing protocols can use different commands.

The following example redistributes the RIP route, whose next hop interface is the fastethernet 0/0, based on the OSPF routing protocol.

```
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)# match interface fastethernet 0/0
```

Related Commands

Command	Description
match ip address	Matches the IP address in the access list.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the source IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

match ip address

Use this command to redistribute a target network route permitted in the access list or the prefix list. Use the **no** form of this command to delete 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: Number of the standard access list ranges from 1 to 99 or from 1300 to 1999. Number of the extended access list ranges from 100 to 199 or from 2000 to 2699.
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Name of the prefix list to be matched

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command can be followed by multiple access list numbers or names.

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

The route-map can be configured very flexibly and applies to the route redistribution and the policy-based routing configuration. No matter how the route-map is used, the configuration principle is the same, except that different command sets are used. Even if the route-map is used for the route redistribution, different routing protocols can use different commands.

The following example shows the redistributed RIP route based on the OSPF routing protocol. It is required that only the RIP routes matching the access list 10 be redistributed. The type of these RIP routes is the external route type-1, and the default metric value is 40 in the OSPF routing area.

Configuration Examples

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# access-list 10 permit 200.168.23.0 0.0.0.255
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip address 10
Ruijie(config-route-map)# set metric 40
Ruijie(config-route-map)# set metric-type type-1
```

Related Commands

Command	Description
access-list	Defines rules for the access list.
match interface	Matches the next-hop interface of the route.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the route source address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

match ip next-hop

Use this command to redistribute a target network route whose next-hop IP address matches rules of the access list or the prefix list. Use the **no** form of this command to delete 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: Number of the standard access list ranges from 1 to 99 or from 1300 to 1999. Number of the extended access list ranges from 100 to 199 or from 2000 to 2699.
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Name of the prefix list to be matched

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command can be followed by multiple access list numbers or names.

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The following example shows the redistributed RIP route based on the OSPF routing protocol. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
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)# access-list 10 permit host 192.168.10.1
Ruijie(config)# access-list 20 permit host 172.16.20.1
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip next-hop 10 20
```

Related Commands

Command	Description
access-list	Defines rules for the access list.
match ip address	Matches the IP address in the access list.
match interface	Matches the next-hop address of the route.
match ip route-source	Matches the route source address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description

N/A

match ip route-source

Use this command to redistribute a target network route whose source IP address matches the access list or the prefix list. Use the no form of this command to delete 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*	Name of the prefix list to be matched

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command can be followed by multiple access list numbers or names.

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The following example shows the redistributed RIP route based on the OSPF routing protocol. As long as the next hop address of the RIP route matches the access list 5, the OSPF allows for redistribution.

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets Ruijie(config-router)#
route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# access-list 5 permit host 192.168.100.1
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip route-source 5
```

Related Commands

Command	Description
access-list	Defines rules for the access list.
match ip address	Matches the IP address in the access list.
match interface	Matches the next-hop interface of the route.
match ip next-hop	Matches the next-hop IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform N/A

Description

match ipv6 address

The goal is to configure filter rules for the IPv6 PBR and use the IPv6 ACL to match packets.

Use this command to define a destination IPv6 route permitted in the redistributed access list or the 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*	Name of the IPv6 prefix list to be matched

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

The sequence number of a route-map can only be added to one Ipv6 ACL.
The sequence number of a route-map is 10 by default.
The Ipv6 PBR function cannot be enabled together with the parameter prefix-list, otherwise, this parameter takes no effect.
You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.
For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.
One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The route-map can be configured very flexibly and applies to the route redistribution and the policy-based routing configuration. No matter how the route-map is used, the configuration principle is the same, except that different command sets are used. Even if the route-map is used for the route redistribution, different routing protocols can use different commands.
The following example shows the redistributed RIP route based on the OSPF routing protocol. It is required that only the RIP routes matching the access list v6acl be redistributed. The default metric value is 30 in the OSPF routing area.

```
Ruijie(config)# ipv6 router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# exit
Ruijie(config)# ipv6 access-list v6acl
```

```
Ruijie(config-ipv6-acl)# 10 permit ipv6 2620::/64 any
Ruijie(config-ipv6-acl)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ipv6 address v6acl
Ruijie(config-route-map)# set metric 30
```

The following example shows steps for configuring the IPv6 PBR function.

Step 1: Configure associated IPv6 ACLs.

```
Ruijie(config)#ipv6 access-list aaa
Ruijie(config-ipv6-acl)#permit ipv6 2003:1000::10/80 2001:100::/64
```

Step 2: Configure match rules for the PBR.

```
Ruijie(config)#route-map user-for-pbr permit 10
Ruijie(config-route-map)#match ipv6 address aaa
```

Related Commands

Command	Description
ipv6 access-list	Defines rules for the IPV6 access list.
match interface	Matches the next-hop interface of the route.
match ipv6 next-hop	Matches the next-hop address in the IPv6 access list.
match ipv6 route-source	Matches the route source address in the IPv6 access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.
set ipv6 default next-hop	Sets the default next-hop IPv6 address for forwarding the packets.
set ipv6 next-hop	Sets the next-hop IPv6 address for forwarding the packets.
show ipv6 policy	Shows the policy-based routing applied on the current device.

Platform Description

RSR20, RSR30, RSR50,and RSR50E

match ipv6 next-hop

Use this command to redistribute a target network route whose next-hop IPv6 address matches rules of the IPv6 access list or 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*	Name of the IPv6 prefix list to be matched

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

The route-map can be configured very flexibly and applies to the route redistribution and the policy-based routing configuration. No matter how the route-map is used, the configuration principle is the same, except that different command sets are used. Even if the route-map is used for the route redistribution, different routing protocols can use different commands.

The following example shows the redistributed RIP route based on the OSPF routing protocol. It is required requires that only the RIP routes matching the access list v6acl be redistributed. The default metric value is 40 in the OSPF routing area.

Configuration Examples

```
Ruijie(config)# ipv6 router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# exit
Ruijie(config)# ipv6 access-list v6acl
Ruijie(config-ipv6-acl)# 10 permit ipv6 2720::/64 any
Ruijie(config-ipv6-acl)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ipv6 next-hop v6acl
Ruijie(config-route-map)# set metric 40
```

Related Commands

Command	Description
ipv6 access-list	Defines rules for the IPV6 access list.
match interface	Matches the next-hop interface of the route.
match ipv6 address	Matches the IP address in the IPv6 access list.
match ipv6 route-source	Matches the route source address in the IPv6 access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the type for the redistributed route.

set tag	Sets the tag for the redistributed route.

Platform Description N/A

match ipv6 route-source

Use this command to redistribute a target network route whose next-hop IPv6 address matches rules of the IPv6 access list or 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*	Name of the IPv6 prefix list to be matched

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

The route-map can be configured very flexibly and applies to the route redistribution and the policy-based routing configuration. No matter how the route-map is used, the configuration principle is the same, except that different command sets are used. Even if the route-map is used for the route redistribution, different routing protocols can use different commands.

Configuration Examples

The following example shows the redistributed RIP route based on the OSPF routing protocol. It is required requires that only the RIP routes matching the access list v6acl be redistributed. The default metric value is 50 in the OSPF routing area.

```
Ruijie(config)# ipv6 router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# exit
Ruijie(config)# ipv6 access-list v6acl
Ruijie(config-ipv6-acl)# 10 permit ipv6 5200::/64 any
Ruijie(config-ipv6-acl)# exit
```

```
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ipv6 route-source v6acl
Ruijie(config-route-map)# set metric 50
```

Related Commands

Command	Description
ipv6 access-list	Defines rules for the IPV6 access list.
match interface	Matches the next-hop interface of the route.
match ipv6 address	Matches the next-hop address in the IPv6 access list.
match ipv6 route-source	Matches the route source address in the IPv6 access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

match length

Use this command to implement the policy-based routing based on the IP packet length in route-map configuration mode. Use the **no** form of this command to delete the setting.

match length *min-length max-length*

no match length *min-length max-length*

Parameter Description

Parameter	Description
min-length	Minimum length of the IP packet
max-length	Maximum length of the IP packet

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

Policy-based routing is a packet forwarding mechanism that is more flexible than the routing based on the target network. After the policy-based routing is used, the device determines how to process the packets to be routed according to the route-map, which determines the next-hop device of the packets.

To apply the policy-based routing, you must specify a route-map to be used by the policy-based routing 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 the 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 a non-default route. The packets that match a policy in the route-map will be processed according to the operation defined in the policy.
To route interactive traffic and mass traffic respectively, use the policy-based routing based on the packet size.

Configuration Examples

The following example enables the policy-based routing on fastethernet 1/0 to send the packets whose size is less than 500 bytes through fastethernet 1/2 interface.

```
Ruijie(config)# interface fastethernet 1/0
Ruijie(config-if)# ip policy route-map smallpak
Ruijie(config-if)# exit
Ruijie(config)# route-map smallpak permit 10
Ruijie(config-route-map)# match length 0 500
Ruijie(config-route-map)# set interface fastethernet 1/2
```

Related Commands

Command	Description
route-map	Defines the route-map.
match ip address	Matches the IP address in the access list.
set default interface	Sets the default output interface for the packets.
set interface	Sets the output interface for the packets.
set ip default next-hop	Sets the default next hop for the packets.
set ip next-hop	Sets the next-hop IP address for the packets.
set ip precedence	Sets the precedence of the IP address for the packets.

Platform Description RSR20, RSR30, RSR50, RSR50E

match metric

Use this command to match a route metric. Use the **no** form of this command to delete the setting.

match metric *metric*

no match metric

Parameter Description

Parameter	Description
metric	Route metric value in the range from 0 to 4294967295

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide You can redistribute a route from one routing process to another routing process. For example, you

can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The following example shows the redistributed RIP route based on the OSPF routing protocol. As long as the metric of the RIP route is 10, the OSPF allows for redistribution.

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redist-rip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redist-rip permit 10
Ruijie(config-route-map)# match metric 10
```

Related Commands

Command	Description
access-list	Defines rules for the access list.
match ip address	Matches the IP address in the access list.
match interface	Matches the next-hop interface of the route.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the route source address in the access list.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description

N/A

match origin

Use this command to redistribute the route whose source IP address is permitted in the access list in route-map configuration mode. Use the **no** form of this command to delete the setting.

match origin {**egp** | **igp** | **incomplete**}

no match origin [**egp** | **igp** | **incomplete**]

Parameter Description

Parameter	Description
egp	EGP from the remote origin.
igp	IGP from the local origin
incomplete	From an incomplete origin.

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide Use this command to set the origin value of a matched route. Only one type of origins of routes can be matched at a time.

Configuration 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	Matches the AS_PATH attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set origin	Sets the type for the redistributed route.

Platform Description N/A

match route-type

Use this command to match the route type of a specified route. Use the **no** form of this command to delete the setting.

match route-type [local | internal | external [type-1 | type-2] | level-1 | level-2 | nssa-external [type-1 | type-2]]

no match route-type [local | internal | external [type-1 | type-2] | level-1 | level-2 | nssa-external [type-1 | type-2]]

Parameter Description

Parameter	Description
local	Locally generated route
internal	OSPF internal route
external	External route (BGP or OSPF external route)
Nssa-external	OSPF NSSA external route
**type-1	type-2**	OSPF external route type 1 or type 2
**level-1	level-2**	IS-IS level-1 or level-2 route

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The following example shows the redistributed OSPF route based on the RIP routing protocol. Only the internal route in the OSPF routing area is redistributed.

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute ospf route-map redrip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match route-type internal
```

Related Commands

Command	Description
access-list	Defines rules for the access list.
match ip address	Matches the IP address in the access list.
match interface	Matches the next-hop interface of the route.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the route source address in the access list.
match metric	Matches the route metric value.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

match tag

Use this command to match the route tag of a specified route. 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

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command can be followed by multiple tags.

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The following example shows the redistributed OSPF route based on the RIP routing protocol. Only the routes with tag 50 and 80 in the OSPF routing area are redistributed.

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute ospf 100 route-map redrip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match tag 50 80
```

Related Commands

Command	Description
access-list	Defines rules for the access list.
match ip address	Matches the IP address in the access list.
match interface	Matches the next-hop interface of the route.
match ip route-source	Matches the route source address in the access list.
match metric	Matches the route metric value.
match ip next-hop	Matches the next-hop IP address in the access list.
match route-type	Matches the route type.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** form of this command to restore the default value.

maximum-paths *number*

no maximum-paths

Parameter Description

Parameter	Description
number	Number of equivalent routes, which is in the range from 1 to 32.

Defaults The default value is 32 for routers. For switches, the default value depends on switch models.

Command Mode Global configuration mode.

Usage Guide

The goal is to control the number of equivalent routes. 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 by executing the **show running config command.**

This command is valid for both the IPv4 and the IPv6. That is, both the maximum number of equivalent paths to an IPv4 destination and the maximum number of equivalent paths to an IPv6 destination are the same value configured in this command.

An equivalent path group indicates multiple equivalent next hops of a prefix. The S8600, S5750, and S7600 switches can support 64 equivalent path groups, and each group supports a maximum of 32 equivalent paths. The S3760 and S5760 switches support a maximum of 8 equivalent paths but without a limit to the equivalent path groups. Namely, each route can support the equivalent paths. If 64 equivalent path groups are configured on the S8600, S5750, and S7600 switches, configuring an equivalent path for a prefix succeeds only when the equivalent path is included in the 64 groups.

Configuration Examples

The following example sets the number of equivalent routes to 10 and then restores it to the default value.

```
Ruijie(config)# maximum-paths 10
Ruijie(config)# no maximum-paths
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

route-map

Use this command to define a route-map and enter the route-map configuration mode. Use the **no** form of this command to delete 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	Defines the name of the route-map. The configuration command for redistributing a routing process references the route-map based on its name. Multiple routing policies can be defined in a route-map, and each policy corresponds to a sequence number.
permit	(Optional) If the keyword permit is defined and the rule defined in the match command is met, the command set controls the redistributed route. For the policy-based routing, the command set controls the packet forwarding, and the system exits the route-map operation. If the keyword permit is defined but the rule defined in the match command is not met, the system performs operations according to the routing policy of the second route-map till the command set is executed.
deny	(Optional) If the keyword deny is defined and the rule defined in the match command is met, no operation is performed. Neither route redistribution nor policy-based routing is supported by the route-map policy, and the system exits the route-map operation. If the keyword deny is defined but the rule defined in the match command is not met, the system performs operations according to the routing policy of the next route-map till the command set is executed.
sequence-number	Sequence number of the route-map policy. The policy with a lower sequence number is preferred, so pay attention to the sequence number setting.

Defaults N/A

Command Mode Global configuration mode

Usage Guide

At present, the RGOS software primarily uses the route-map for route redistribution control and policy-based routing.

1. Route redistribution control

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match**

command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

When configuring route-maps, pay attention to the following aspects:

When you create the first route-map policy, if the sequence-number is not specified, it is 10 by default;

If only one route-map policy is available and the 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 must be specified; otherwise an error message will be displayed.

Configuration Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the number of the redistribution hops counting 4. In the OSPF route domain, the route type of the RIP routes is the external route type-1, the default metric value is 40, and the tag is 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)# match metric 4
Ruijie(config-route-map)# set metric 40
Ruijie(config-route-map)# set metric-type type-1
Ruijie(config-route-map)# set tag 40
```

Related Commands

Command	Description
redistribute	Redistributes the routes.

Platform Description N/A

send-lifetime

Use this command to specify the lifetime of an encryption key in its sending direction in encryption key configuration mode. 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 of the encryption key. 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—date 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 lifetime of the encryption key. It must be later than the start time.
duration *seconds*	Duration of the encryption key from the start time. The value ranges from 1 to 2147483646.

Default infinite

Command Mode Encryption key configuration mode

Usage Guide Use this command to specify the lifetime of an encryption key in its sending direction.

Configuration 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)# key 1
Ruijie(config)# send-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

set aggregator as

Use this command to specify the AS_PATH attribute value for the aggregator of the specified routes that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting. This command applies only to policy-based routing configuration.

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 The 10.4(3) or later version supports the AS number with four bytes. The added AS number ranges from 1

	to 4294967295, and 1 to 65535.65535 in dot mode.
ip_address	IP address of the aggregator

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide Use this command to set the AS_PATH attribute for the matched routes in the BGP routing area. Only one group of parameters (as-number, ip-addr) is allowed to be configured at a time.

Configuration 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	Matches the AS_PATH attribute of the route.
match community	Matches the route community.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set community	Sets the COMMUNITY attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the type for the redistributed route.

Platform Description N/A

set as-path prepend

Use this command to add the specified AS_PATH attribute value for the routes that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting. This command applies only to the policy-based routing configuration.

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 added. The 10.4(3) or later version supports the AS number with four bytes. The added AS number ranges from 1 to 4294967295, and 1 to 65535.65535 in dot mode.

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide Use this command to add the specified AS_PATH attribute for the matched routes. Up to 15 ASs can be added into the as-path at a time.

Configuration 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	Matches the AS_PATH attribute of the route.
match community	Matches the route community.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set community	Sets the COMMUNITY attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the type for the redistributed route.

Platform Description N/A

set comm-list delete

Use this command to delete all COMMUNITY attribute values in the COMMUNITY_LIST for the routes that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting. This command applies only to the policy-based routing configuration.

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: The Number of the standard community list ranges from 1 to 99. The Number of the expanded community list ranges from 100 to 199.
community-list-name	Name of the community list, which should not exceed 80 characters.

Defaults N/A

Command Route-map configuration mode

Mode

Usage Guide Use this command to delete the COMMUNITY attribute value for a matched route.

Configuration 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
ip community-list	Matches the community list.
match as-path	Matches the AS_PATH attribute value of the route.
match community	Matches the COMMUNITY attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set comm-list delete	Deletes the matched COMMUNITY attribute value.
set local-preference	Sets the local preference for the redistributed route.

Platform Description N/A

set community

Use this command to specify a COMMUNITY attribute value for a route that meets the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

set community {*community-number[community-number* …] **additive** | **none**}

no set community

Parameter Description

Parameter	Description
community-number	COMMUNITY attribute value in the format of AA:NN (AS number:2-byte numerical) or a value in the range from 0 to 4294967295. It may also be one of the following pre-defined value:

	internet: indicates the Internet community. All paths belong to this community. local-as: indicates that this path will be advertised within the AS. After AS confederation is configured, this path will not be advertised to other ASs or sub-ASs. no-advertise: indicates that this path will not be advertised to any BGP peers. no-export: indicates that this path will not be advertised to any EBGP peers.
additive	Increases based on the original COMMUNITY attribute.
none	Sets the COMMUNITY attribute as blank.

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide Use this command to set the COMMUNITY attribute for a matched route.

Configuration 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	Matches the AS_PATH attribute value of the route.
match community	Matches the COMMUNITY attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set origin	Sets the source for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.

Platform Description N/A

set dampening

Use this command to specify the dampening parameter for a route that meets the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

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 from 1 to 45 minutes, with 15 minutes as the default value.
reuse	When the route penalty is lower than this value, the route suppression is released. The value is in the range from 1 to 20000, with 750 as the default value.
suppress	When the route penalty is higher than this value, the route is suppressed. The value is in the range from 1 to 20000, with 2000 as the default value.
max-suppress-time	Maximum duration for suppressing a route, which is in the range from 1 to 255 minutes, with 4* as the default value of the half-life.

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide Use this command to specify the dampening parameter for a matched route.

Configuration 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	Matches the AS_PATH attribute value of the route.
match community	Matches the COMMUNITY attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set local-preference	Sets the local preference for the redistributed route.

Platform Description N/A

set default interface

Use this command to specify the default interface for forwarding the packets whose route meets the match rule but without an egress in route-map configuration mode. Use the **no** form of this command to delete the setting.

set default interface *interface-type interface-number* […*interface-type interface-number*]

no set default interface *interface-type interface-number* […*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type	Interface type.
interface-number	Interface ID.

Default N/A

Command Mode Route-map configuration mode

Usage Guide

This command can be followed by multiple interfaces.

Policy-based routing is a packet forwarding mechanism that is more flexible than the routing based on the target network. After the policy-based routing is used, the device determines how to process the packets to be routed according to the route-map, which determines the next-hop device of the packets.

To apply the policy-based routing, you must specify a route-map to be used by the policy-based routing 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 the 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 a non-default route. The packets that match a policy in the route-map will be processed according to the operation defined in the policy.

If the state of the first configured interface is down, the system may attempt to use the second interface set by the command set. A route-map policy may contain multiple set operations.

Configuration Examples

The following example enables the policy-based routing on serial 1/0 to send the packets through the fastEthernet 1/0 interface when packets whose size is less than 500 bytes are received and the route is not defined in the routing table.

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# ip policy route-map smallpak
Ruijie(config-if)# exit
Ruijie(config)# route-map smallpak permit 10
Ruijie(config-route-map)# match length 0 500
Ruijie(config-route-map)# set default interface fastethernet 1/0
```

Related Commands

Command	Description
route-map	Defines a route-map.
match ip address	Matches the IP address in the access list.

match length	Matches the range of the packet length.
set interface	Sets the output interface for the packets.
set ip default next-hop	Sets the default next hop for the packets.
set ip next-hop	Sets the next-hop IP address for the packets.
set ip precedence	Sets the precedence of the IP address for the packets.

Platform Description N/A

set extcommunity

Use this command to specify the expanded community attribute value for a route that meets the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting. This command applies only to policy-based routing configuration.

set extcommunity {**rt** *extend-community-value* | **soo** *extend-community-value*}

no set extcommunity {rt | soo }

Parameter Description

Parameter	Description
rt	Specifies the RT attribute value for the route.
soo	Specifies the SOO attribute value for the route.
extend-community-value	Expanded community value: Three types of extend_community_value parameters are as follows: (1) extend_community _value=as_num: nn The as_num is a public AS number with two bytes. The nn ranges from 0 to 4294967295, which is defined by the user. (2) extend_community_value=ip_addr: nn The ip_addr must be a global IP address. The nn ranges from 0 to 65535, which is defined by the user. (3) extend_community_value=as4_num: nn The as_num is a public AS number with four bytes. The nn ranges from 0 to 65535, which is defined by the user.

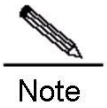
Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

Use this command to set the expanded community attribute for a matched route.
The 10.4(3) or later version adds the function of configuring the AS4 expanded community attribute and allows to configure the AS expanded community attribute with four bytes. The format of the AS expanded community attribute with four bytes is AS4:NN. The AS4 number can be presented with

decimal digits or in dot mode. It ranges from 1 to 4294967295 in the decimal system or 1 to 65535.65535 in dot mode. The nn ranges from 0 to 65535.



Note

The AS4 number ranges from 1 to 65535 both in the decimal system and in dot mode. Therefore, it is saved as the AS number with two bytes.

Configuration 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	Matches the AS_PATH value of the route.
match community	Matches the community value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.

Platform Description N/A

set fast-reroute

Use this command to specify a backup egress interface and backup next hop for the fast reroute matching rules. 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	Specifies a backup egress interface.
ip-address	Specifies a backup next hop (mandatory for a non-P2P interface).

Defaults Disabled

Command mode Route map configuration mode

Usage Guide This command is used to configure an backup egress interface and next hop for an IP fast reroute.

The current software version only supports one backup route and this command support only configuration of one set of interface and next hop parameters.
This command is used exclusively to configure the fast reroute.


Caution The IP fast reroute should not be a directly connected route or local route.

Configuration Examples The following example specifies a backup egress interface and backup next hop for the fast reroute matching rules.

```
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 Commands

Command	Description
match ip-address	Matches with the ACL.

Platform Description N/A

set interface

Use this command to specify the interface for forwarding the packets that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

set interface *interface-type interface-number* [*…interface-type interface-number*]

no set interface *interface-type interface-number* [*…interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type	Interface type.
interface-number	Interface ID

Default N/A

Command Mode Route-map configuration mode

Usage Guide This command can be followed by multiple interfaces.
Policy-based routing is a packet forwarding mechanism that is more flexible than the routing based on the target network. After the policy-based routing is used, the device determines how to process the packets to be routed according to the route-map, which determines the next-hop device of the

packets.

To apply the policy-based routing, you must specify a route-map to be used by the policy-based routing 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 the 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 a non-default route. The packets that match a policy in the route-map will be processed according to the operation defined in the policy.

If the state of the first configured interface is down, the system may attempt to use the second interface set by the command set. A route-map policy may contain multiple set operations.

If the interface is set to null 0, the packets will be discarded.

Configuration Examples

The following example enables the policy-based routing on the serial 1/0 interface to send packets through the fastethernet 0/0 interface when the size of the received packets is less than 500 bytes.

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#ip policy route-map smallpak
Ruijie(config)#route-map smallpak permit 10
Ruijie(config-route-map)#match length 0 500
Ruijie(config-route-map)#set interface fastethernet 0/0
```

Related Commands

Command	Description
route-map	Defines a route-map.
match ip address	Matches the IP address in the access list.
match length	Matches the range of the packet length.
set default interface	Sets the default output interface for the packets.
set ip default next-hop	Sets the default next hop for the packets.
set ip next-hop	Sets the next-hop IP address for the packets.
set ip precedence	Sets the precedence of the IP address for the packets.

Platform Description

N/A

set ip default next-hop

Use this command to specify the default next-hop IP address for packets that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete 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

Defaults

N/A

Command Mode Route-map configuration mode

This command supports the WCMP load balancing mode and non-WCMP load balancing mode. In WCMP load balancing mode, the system implements WCMP load balancing according to the weight input by users.

This command supports up to 32 IP addresses.

If a weight is added to an IP address, up to four next-hop IP addresses can be configured.

Note

If a weight follows any next-hop IP address, the operation mode of this command will automatically switches to the WCMP load balancing mode. Under this mode, the weight of those next-hop IP addresses whose weights are not configured is 1 by default.

Usage Guide

Differences between the **set ip next-hop** and **set ip default next-hop** commands are as follows: For the system configured the **set ip next-hop** command, the policy-based routing takes precedence for forwarding packets; while for the system configured the **set ip default next-hop** command, the routing and forwarding table takes precedence for forwarding packets.

Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packets will be forwarded to the next hop configured in this command.

To apply the policy-based routing, you must specify a route-map to be used by the policy-based routing 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 the 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 a non-default 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.

Configuration Examples

The following example forwards the packets from two different nodes through different routes.

For the packets received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to the device 6.6.6.6. For the packets received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to the device 7.7.7.7. Other packets 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
Ruijie(config- route-map)#set default interface null 0
```

Related Commands

Command	Description
route-map	Defines a route-map.
match ip address	Matches the IP address in the access list.
set default interface	Sets the default output interface for the packets.
set interface	Sets the output interface for the packets.
set ip next-hop	Sets the next–hop IP address for the packets.
set ip precedence	Sets the precedence of the IP address for the packets.

Platform Description N/A

set ip dscp

Use this command to specify the DSCP value for packets that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

set ip dscp *dscp-value*

no set ip dscp

Parameter Description

Parameter	Description
dscp-value	Specifies the DSCP value for the IP header in the IP packets.

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
route-map	Defines a route-map.
match ip address	Matches the IP address in the access list.
set default interface	Sets the default output interface for the packets.
set interface	Sets the output interface for the packets.
set ip next-hop	Sets the next-hop IP address for the packets.
set ip precedence	Sets the precedence of the IP address for the packets.

Platform Description N/A

set vrf

Use this command to route IP packets that meet the match rule according to the specified VRF routing table. Use the **no** form of this command to delete the setting. This command applies only to policy-based routing configuration.

set vrf *name*

no set vrf *name*

Parameter Description	**Parameter**	**Description**
	name	Name of the VRF instance

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

Use this command to route and forward the IP packets that meet different match rules according to different VRF routing tables.

If the uni-protocol IPv4 VRF is specified, the IPv6 PBR takes no effective.

If the multi-protocol VRF without IPv4 address family is specified, the IPv4 PBR takes no effect. If the multi-protocol VRF without IPv6 address family is specified, the IPv6 PBR takes no effective. If the multi-protocol VRF with the IPv4 and IPv6 address families is specified, this command is valid for the IPv4 PBR and IPv6 PBR.

Note

1. Before configuring this command, the VRF must exist. If the specified VRF does not exist, the system prompts error message. After the VRF instance is deleted, the setting that uses this VRF instance is also deleted.

- If the VRF specified in this command does not exist, the system prompts:
  %route-map: VRF table vrf-name does not exist.
- If the corresponding set vrf configuration in the route-map is deleted at the same time when the VRF is deleted, the system prompts:
  %route-map: set vrf vrf-name configuration removed from all route-maps.

Note

2. The same policy of the route-map does not allow to configure the **set vrf** and **set ip next-hop** commands, or the **set vrf** and **set ip next-hop verify-availability** commands at the same time. However, the **set vrf** and **set ip tos** commands, the **set vrf** and **set ip precedence** commands, or the **set vrf** and **set ip dhcp** commands can be configured at the same time. If the **set vrf** command is executed many times based on the same policy of the route-map, the later configuration will overwrite the previous configuration without any prompt.

Based on the same policy of the route-map:

- If the **set ip nexthop** command is configured before the set vrf command, the system prompts:
  % route-map: cannot set vrf .
  % Remove other set clauses to set vrf.
- If the **set vrf** command is configured before the set ip nexthop command, the system prompts:
  % route-map: cannot set next-hop.
  % Remove set vrf clause before set ip next-hop.

From the version 10.4(3), the **set vrf**, **set ip nexthop** and **set ipv6 next-hop** commands can be configured based on the same policy of the route-map at the same time. The **set vrf** command takes precedence over the **set ip nexthop** and **set ipv6 next-hop** commands.

Configuration Examples

The following example enables the policy-based routing on the interface serial 1/0. When the interface receives the packets from the source address that ranges from 10.0.0.0 to 10.0.0.8, the packets will be forwarded through the route based on the vrf_A routing table. When the interface receives the packets from the source address that ranges from 172.16.0.0 to 172.16.0.16, the packets will be forwarded through the route based on the vrf_B routing table. All other packets will be forwarded through the route based on the global routing table.

The specific operations are as follows:

Step 1: Define the ACL to be used.

```
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
```

Step 2: Configure the route-map.

```
Ruijie(config)#route-map PBR permit 10
Ruijie(config-route-map)#match ip address 10
Ruijie(config-route-map)#set vrf vrf_A
Ruijie(config)#route-map PBR permit 20
Ruijie(config-route-map)#match ip address 20
Ruijie(config-route-map)#set vrf vrf_B
```

Step 3: Configure the policy-based routing on the interface.

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#ip policy route-map PBR
```

Step 4: Configure an ip vrf receive route on the interface for each VRF to be selected and add the IP address of the interface into the VRF.

```
Ruijie(config-if)#ip vrf receive vrf_A
Ruijie(config-if)#ip vrf receive vrf_B
```

Related Commands

Command	Description
route-map	Defines a route-map.
match ip address	Matches the IP address in the access list.
match length	Matches the length of the IP packets.
ip vrf receive	Imports the direct-connection route and host route of an interface to the VRF routing table specified in vrf_name.
vrf receive	Imports the local IPv4 or IPv6 host route and direct-connection route of an interface to the VRF routing table specified in vrf_name.

Platform Description

N/A

set ip next-hop

Use this command to specify the next-hop IP address for packets that match the match rule. Use the **no** form of this command to delete the setting. This command applies only to policy-based routing configuration.

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

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command supports the WCMP load balancing mode and non-WCMP load balancing mode. In WCMP load balancing mode, the system implements WCMP load balancing according to the weight input by users.

This command supports up to 32 IP addresses.

If a weight is added to an IP address, up to four next-hop IP addresses can be configured.

Note

If a weight follows any next-hop IP address, the operation mode of this command will automatically switches to the WCMP load balancing mode. Under this mode, the weight of those next-hop IP addresses whose weights are not configured is 1 by default.

Policy-based routing is a packet forwarding mechanism that is more flexible than the routing based on the target network. After the policy-based routing is used, the device determines how to process the packets to be routed according to the route-map, which determines the next-hop device of the packets. To apply the policy-based routing, you must specify a route-map to be used by the policy-based routing 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 the 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 a non-default 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.

Configuration Examples

The following example enables the policy-based routing on the interface serial 1/0. When the interface receives the packets from the source address that ranges from 10.0.0.0 to 10.0.0.8, the packets will be sent to 192.168.100.1. When the interface receives the packets from the source address that ranges from 172.16.0.0 to 172.16.0.16, the packets will be sent to 172.16.100.1. All other packets will be discarded.

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#ip policy route-map load-balance
Ruijie(config)#access-list 10 permit 10.0.0.0 0.255.255.255
Ruijie(config)#access-list 20 permit 172.16.0.0 0.0.255.255
Ruijie(config)#route-map load-balance permit 10
Ruijie(config-route-map)#match ip address 10
Ruijie(config-route-map)#set ip next-hop 192.168.100.1
Ruijie(config)#route-map load-balance permit 20
Ruijie(config-route-map)#match ip address 20
Ruijie(config-route-map)#set ip next-hop 172.16.100.1
Ruijie(config)#route-map load-balance permit 30
Ruijie(config-route-map)#set interface Null 0
```

Related

Command	Description

Commands

route-map	Defines a route-map.
match ip address	Matches the IP address in the access list.
set default interface	Sets the default output interface for the packets.
set interface	Sets the output interface for the packets.
set ip default next-hop	Sets the default next–hop IP address for the packets.
set ip precedence	Sets the precedence of the IP address for the packets.

Platform Description N/A

set ip next-hop verify-availability

Use this command to verify the availability of the next-hop IP address. Use the **no** form of this command to delete the setting. This command applies only to policy-based routing configuration.

set ip next-hop verify-availability *ip-address* **track** *track-object-num*

no set ip next-hop verify-availability *ip-address* **track** *track-object-num*

Parameter Description

Parameter	Description
ip-address	IP address of the next hop
track-obj-num	Number of the object to be tracked

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide N/A

Configuration Examples The following example verifies the availability of the next-hop IP address 192.168.1.2. The number of the object to be tracked is 1.

```
Ruijie(config)#route-map rmap permit 10
Ruijie(config-route-map)#set ip  next-hop verify-availability 192.168.1.2
track 1
```

Related Commands

Command	Description
route-map	Defines a route-map.
match ip address	Matches the IP address in the access list.
set default interface	Sets the default output interface for the packets.
set interface	Sets the output interface for the packets.
set ip default next-hop	Sets the default next-hop IP address for the packets.
set ip precedence	Sets the precedence of the IP address for the packets.

Platform Description N/A

set ip precedence

Use this command to set the precedence of the IP headers for packets that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

set ip precedence {*<0-7>* | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ip precedence

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

The IP packets routed based on the policy-based routing are usually sent by configuring different precedence values for the IP packet headers

The route-map configuration rule allows you to configure multiple **set ip precedence** commands, but only the last configuration takes effect, and the precedence will be specified for the IP header of the packet that matches the PBR rule.

Configuration Examples

The following example sets the precedence for the packet with the source IP address 192.168.217.68 from the interface FastEthernet 0/0 to 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	Matches the next-hop interface of the route.
match ip address	Matches the IP address in the access list.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the route source IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

set ip tos	Sets the ToS for the IP packet header.

Platform Description N/A

set ip tos

Use this command to set the ToS of the IP headers for packets that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

set ip tos {*<0-15>* | *max-reliability* | *max-throughput* | *min-delay* | *min-monetary-cost* | *normal* }

no set ip tos

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

The IP packets routed based on the policy-based routing are usually sent by configuring different ToS values for the IP packet headers.
The ToS value will be specified for the IP header of the packet that matches the PBR rule.

Configuration Examples

The following example sets the ToS value for the packet with the source IP address 192.168.217.68 from the interface FastEthernet 0/0 to 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	Matches the next-hop interface of the route.
match ip address	Matches the IP address in the access list.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the route source IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.

set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.
set ip precedence	Sets the precedence for the IP packet header.

Platform Description N/A

set ipv6 default next-hop

Use this command to specify the default next-hop IPv6 address for IPv6 packets that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting. This command applies only to policy-based routing configuration.

set ipv6 default next-hop *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*]...]

no set ipv6 default next-hop *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*]...]

Parameter Description

Parameter	Description
global-ipv6-address	IPv6 address of the next hop for forwarding the packets. The next-hop router must be an adjacent router
weight	Weight in load balancing mode, which is in the range from 1 to 8

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

After the policy-based routing is applied to the interface, for the IPv6 packets matching corresponding rules, if the routing table does not include the non-default route with the destination of the packets, the packets will be forwarded to the next hop specified in the **set ipv6 default next-hop** command. Otherwise, is the packets will be forwarded through the non-default route. Noted that the match rule should be an IPv6-associated rule.

Packets select the egress from the policy-based routing and routing table with the following priority:

- set ipv6 next-hop;
- non-default route;
- set ipv6 default next-hop
- default route.

For the switches, this function does not take effect if the mask length exceeds 64 network segments.

If this command and the set ipv6 next-hop verify-availability command are configured at the same time, the next hop set in the set ipv6 next-hop verify-availability command

takes precedence.

Configuration Examples

The following example sets the default next hop for the packet with the destination IP address 2001:0db8:2001:1760::/64 from the interface fastEthernet 0/0 to 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	Sets the match rule of the policy-based routing.
ipv6 policy route-map	Applies the policy-based routing on the interface.
set ipv6 next-hop	Sets the next hop IPv6 address of the policy-based routing.

Platform Description

This command is supported on the RSR20, RSR30, RSR50, and RSR50E series routers.

set ipv6 next-hop

Use this command to specify the next-hop IPv6 address for packets that meet the match rule. Use the no form of this command to delete the setting. This command applies only to policy-based routing configuration.

set ipv6 [**vrf** *vrf-name* | **global**] **next-hop** *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*]...]

no set ipv6 [**vrf** *vrf-name* | **global**] **next-hop** *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*]...]

Parameter Description

Parameter	Description
vrf *vrf-name*	The next hop belongs to the specified VRF which must be a multi-protocol VRF of the configured IPv6 address family.
global	The next hop belongs to the global VRF.
global-ipv6-address	IPv6 address of the next hop for forwarding the packets. The next-hop router must be an adjacent router.
weight	Weight of the next hop in load balancing mode, which is in the range from 1 to 8.

Defaults

N/A

Command Mode

Route-map configuration mode

Usage Guide

This command supports the WCMP load balancing mode and non-WCMP load balancing mode. In WCMP load balancing mode, the system implements WCMP load balancing according to the weight input by users.

This command supports up to 32 IP addresses.

If a weight is added to an IP address, up to four next-hop IP addresses can be configured.

If the parameter **vrf** *vrf-name* is specified, the packets will be forwarded across the VRFs. If the parameter **global** is specified, the packets will be forwarded from the VRF to the public network. If no [**vrf** *vrf-name* | **global**] is specified, the default VRF is used when the IPv6 packets are forwarded, that is, the next hop belongs to the VRF that receives the IPv6 packets.


Caution

If a weight follows any next-hop IP address, the operation mode of this command will automatically switches to the WCMP load balancing mode. Under this mode, the weight of those next-hop IP addresses whose weights are not configured is 1 by default.

Packets select the egress from the policy-based routing and routing table with the following priority:

- set ipv6 next-hop;
- non-default route;
- set ipv6 default next-hop;
- Default route.

Configuration Examples

The following example sets the next hop for the packet with the destination IP address 2001:0db8:2001:1760::/64 from the interface fastEthernet 0/0 to 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	Sets the match rule of the policy-based routing.
ipv6 policy route-map	Applies the policy-based routing on the interface.
set ipv6 next-hop	Sets the next hop IPv6 address of the policy-based routing.

Platform Description

This command is supported on the RSR20, RSR30, RSR50, and RSR50E series routers.

set ipv6 precedence

Use this command to set the precedence of the IPv6 headers for packets that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the 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 value of the IPv6 packet header
0~7	In the range from 0 to 7

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

The following table shows the mappings between the value and type.

Value	Type
0	routine
1	priority
2	network
3	internet
4	immediate
5	flash-override
6	flash
7	critical

Configuration Examples

The following example sets the precedence of the IPv6 packet header to 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 the 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	Configures the ACL used for matching the packets in the IPv6 PBR table.
route-map	Configures the route-map that applies the policy-based routing.
set default interface	Sets the default next-hop egress.
set interface	Sets the next-hop egress.

set ipv6 default next-hop	Sets the default next-hop address for forwarding the packets.
set ipv6 next-hop	Sets the next-hop address for forwarding the packets.
show ipv6 policy	Shows the policy-based routing applied on the current device.
show route-map	Shows the current route-map configuration.

Platform Description N/A

set level

Use this command to specify the level of the target area for routes that meet the match rule. Use the **no** form of this command to delete the setting.

set level {**level-1**| **level-2** | **level-1-2** | **stub-area** | **backbone**}

no set level

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide N/A

Configuration Examples

The following example shows that the RIP route is redistributed to the backbone area based on the OSPF routing protocol.

```
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	Matches the next-hop interface of the route.
match ip address	Matches the IP address in the access list.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the source IP address in the access list.
match metric	Matches the route metric value.

match route-type	Matches the route type.
match tag	Matches the route tag.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

set local-preference

Use this command to set the LOCAL_PREFERENCE value for routes that meet the match rule. Use the **no** form of this command to delete the setting.

set local-preference *number*

no set local-preference

Parameter Description

Parameter	Description
number	Local preference metric, which ranges from 1 to 4294967295.

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide Use this command to set the local preference for the matched routes. Only one local-preference value can be set.

Configuration 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	Matches the AS_PATH attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.

set metric-type	Sets the metric type for the redistributed route.

Platform Description N/A

set metric

Use this command to set the metric value for routes that meet the match rule. Use the **no** form of this command to delete the setting.

set metric [+ *metric-value* | - *metric-value* | *metric-value*]

no set metric

Parameter Description

Parameter	Description
+	Increases based on the metric of the original route.
-	Decreases based on the metric of the original route.
metric-value	Specifies the metric value for the redistributed route

Defaults The default metric value for the redistributed route varies with the routing protocol.

Command Mode Route-map configuration mode

Usage Guide

You should set the metric according to the actual network topology, because the routing depends on the route metric values. 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 increasing or decreasing a value is from 1 to 16.

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The following example shows the redistributed RIP route based on the OSPF routing protocol. The default metric value is set to 40 for the redistributed route.

```
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	Matches the next-hop interface of the route.
match ip address	Matches the IP address in the access list.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the source IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

set metric-type

Use this command to set the metric type for routes that meet the match rule. Use the **no** form of this command to delete the setting.

set metric-type *type*

no set metric-type

Parameter Description

Parameter	Description
type	Type of the redistributed route

Defaults The type of the OSPF redistributed route is set to Type 2 by default.

Command Mode Route-map configuration mode

Usage Guide

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is performed.

Configuration Examples

The following example shows the redistributed RIP route based on the OSPF routing protocol. The type of the redistributed route is set to 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	Matches the next-hop interface of the route.
match ip address	Matches the IP address in the access list.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the source IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description N/A

set next-hop

Use this command to specify the next-hop IP address for routes that meet the match rule. Use the **no** form of this command to delete the setting. This command applies only to the configuration of routing policies.

set next-hop *ip-address*

no set next-hop

Parameter Description

Parameter	Description
ip-address	IP address of the next hop

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

You can redistribute a route from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing area and then advertise it to the RIP routing area, and vice versa. All IP routing protocols support the mutual route redistribution.

For route redistribution, route-maps are usually used to control the mutual route redistribution between two routing areas.

One or more **match** or **set** commands can be executed to configure a route-map. If the **match** command is not used, all routes are matched. If the **set** command is not used, no operation is

performed.

Configuration Examples

The following example sets the next-hop IP address for the route that matches the access list 1 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	Matches the next-hop interface of the route.
match ip address	Matches the IP address in the access list.
match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the source IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric-type	Sets the metric type for the redistributed route.
set tag	Sets the tag for the redistributed route.

Platform Description

N/A

set origin

Use this command to set the origin attribute for routes that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

set origin {**egp** | **igp** | **incomplete**}

no set origin

Parameter Description

Parameter	Description
egp	EGP from remote origin
igp	IGP from local origin
incomplete	Unknown origin

Defaults

N/A

Command Mode

Route-map configuration mode

Usage Guide

Use this command to set the origin attribute for the matched routes. Only one origin attribute for the routes can be set.

Configuration 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	Matches the AS_PATH attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set local-preference	Sets the local preference for the redistributed route.

Platform Description N/A

set originator-id

Use this command to set the origin attribute for routes that meet the match rule in route-map configuration mode. Use the **no** form of this command to delete the setting.

set originator-id *ip-addr*

no set originator-id [*ip-addr*]

Parameter Description

Parameter	Description
ip-addr	IP address of the originator

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide Use this command to set the origin attribute for the matched routes.

Configuration 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	Matches the AS_PATH attribute value of the route.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.
set as-path prepend	Sets the AS_PATH attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set local-preference	Sets the local preference for the redistributed route.

Platform Description N/A

set tag

Use this command to set the tag for routes that meet the match rule. Use the **no** form of this command to delete the setting.

set tag *tag*

no set tag

Parameter Description

Parameter	Description
tag	Tag of the redistributed route

Defaults The original route tag remains unchanged.

Command Mode Route-map configuration mode

Usage Guide This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

Configuration Examples

The following example shows the redistributed RIP route based on the OSPF routing protocol. The tag of the redistributed route is set to 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	Matches the next-hop interface of the route.
match ip address	Matches the IP address in the access list.

match ip next-hop	Matches the next-hop IP address in the access list.
match ip route-source	Matches the source IP address in the access list.
match metric	Matches the route metric value.
match route-type	Matches the route type.
match tag	Matches the route tag.
set metric	Sets the metric value for the redistributed route.
set metric-type	Sets the metric type for the redistributed route.

Platform Description N/A

set weight

Use this command to set the weight value for a BGP route that meets the match rule. Use the **no** form of this command to delete the setting.

set weight *number*

no set weight

Parameter Description

Parameter	Description
number	Weight value in the range from 0 to 65535

Defaults N/A

Command Mode Route-map configuration mode

Usage Guide

This command can only be used to modify the weight value of a BGP route.
By default, the weight value of the route learned from a neighbor is the one configured in the neighbor weight command. The weight value of the locally generated route is fixed to 32768.

Configuration Examples

The following example sets the weight value for the BGP route learned from the neighbor 1.1.1.1 in 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	Matches the AS_PATH attribute of the route.
match community	Matches the route community value.
match metric	Matches the route metric value.
match origin	Matches the origin value of the route.

set community	Sets the COMMUNITY attribute for the redistributed route.
set metric	Sets the metric value for the redistributed route.
set metric type	Sets the metric type for the redistributed route.

Platform Description N/A

show ip community-list

Use this command to show information about a community list.

show ip community-list [*community-list-number* | *community-list-name*]

Parameter	Description
community-list-number	Number of the community list: The number of the standard community list ranges from 1 to 99. The number of the expanded community list ranges from 100 to 99.
community-list-name	Name of the community list, which should not exceed 80 characters.

Parameter Description

Defaults N/A

Command Mode Privileged mode

Usage Guide This command is used to show the information about the community list.

Configuration Examples

```
Ruijie# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

Command	Description
match community	Matches the community list.
set comm-list delete	Deletes the COMMUNITY attribute value of the BGP route attribute based on the community list.

Related Commands

Platform Description N/A

show ip prefix-list

Use this command to view information about a prefix list or entries in the prefix list.

show ip prefix-list [*prefix-name*]

Parameter Description

Parameter	Description
prefix-name	Name of the prefix list

Defaults The configuration information about all prefix lists is displayed by default.

Command Mode Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and route-map configuration mode.

Usage Guide If no prefix list is specified, the configurations of all prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Configuration Examples

```
Ruijie# show ip prefix-list
ip prefix-list pre: 2 entries
seq 5 permit 192.168.64.0/24
seq 10 permit 192.2.2.0/24
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip route

Use this command to view information about an IP routing table.

show ip route [[**vrf** *vrf_name*] [*network* [*mask*] | **count** | *protocol* [*process-id*] | **weight**]]

Parameter Description

Parameter	Description
vrf *vrf_name*	(Optional) Only shows the route information about the VRF.
network	(Optional) Only shows the route information to the target network.
mask	(Optional) Only shows the route information to the target network of the mask.
count	(Optional) Shows the number of current routes. (Count one route for the ECMP or WCMP route.)
protocol	(Optional) Shows the routing protocol or the keyword connected or static. When specific protocol routes are displayed, use the keywords bgp, isis, ospf, and rip.

process-id	(Optional) Process ID of a routing protocol
weight	(Optional) Only shows the non-default-weight routes.
normal	Displays only the common route.
ecmp	Displays only the equal-cost multi-path route.
fast-reroute	Didsplays only the fast reroute

Defaults All routes are displayed by default.

Command Mode Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and route-map configuration mode.

Usage Guide This command can be used to show specified route information flexibly based on specified options. The **show ip route command** is used to display available entries for forwarding. If you want to view entries of other routes, please set the **normal**, **ecmp** and **fast-reroute** parameters.

Configuration Examples

The following example shows the output of this command:

```
Ruijie# show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
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
i - IS-IS,su - IS-IS summary,L1 - IS-IS level-1,L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate defaultGateway 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.
```

The following example shows the output of the **show ip route** *network* command:

```
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
```

The following example shows the output of the **show ip route count** command:

```
Ruijie# show ip route count
--------- route info ----------
the num of active route: 5
```

The following example shows the output of the **show ip route weight** command:

```
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
```

The following example shows the output of the **show ip route normal** command.

```
Ruijie#show ip route normal
Codes:  C - connected, S - static, R - RIP, B - BGP
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
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS 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
```

The following example shows the output of the **show ip route ecmp** command.

```
Ruijie#show ip route ecmp
Codes:  C - connected, S - static, R - RIP, B - BGP
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
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS 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
```

The following example shows the output of the **show ip route fast-reroute** command.

```
Ruijie#show ip route fast-reroute
Codes:  C - connected, S - static, R - RIP, B - BGP
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
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS 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
```

The following example shows the output of the **show ip route fast-reroute** *network* command.

```
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
```

The output of this command is described as follows:

Field	Description
O	Source routing protocol of the route, 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 route type 1 N2: OSPF NSSA external route type 2 IA: internal route in the OSPF routing area SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route ia: internal route in the IS-IS routing area
20.0.0.0/8	Network address and mask of the target network
[1/0]	Management distance/metric value
Via 20.0.0.1	Next-hop IP address
00:00:06	Time to live (TTL)
VLAN 1	Forwarding interface of the next hop
Routing Descriptor Blocks	Displays the next IP address, route source, update time, interfaces passed through, source routing protocol, type and Border Gateway Protocol (BGP) community value.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip route summary

Use the following command to view the statistical information about a single routing table.

show ip route [**vrf** *vrf_name*] **summary**

Use the following command to view the statistical information about all routing tables.

show ip route summary all

Parameter Description

Parameter	Description
vrf-name	VRF name

Defaults N/A

Command Mode Privileged user mode

Usage Guide N/A

Configuration Examples

The following example shows the statistical information about 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 shows the statistical information about 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
        Static      2       1       1       4
        RIP         1       2       1       4
        OSPF        2       1       1       4
        ISIS        1       2       0       3
        BGP         2       1       1       4
        TOTAL       11      7       4       22
```

Field	Description
NORMAL	Specifies the entry type. You can fill in this field with one of the following parameters: NORMAL: Common routing entries (non ECMP or FRR routing entries) ECMP: Equal-cost multi-path routing entries FRR: Fast reroute routing entries TOTAL: All entries of various types

Memory	Memory consumed by the current routing table.
Entries	Entries contained within the current routing table (prefix-based entries instead of next hop entries)
Connected	Specifies the protocol type of this entry. You can fill in this field with one of the following parameters: Connected: Connected routing entries Static: Static routing entries RIP: RIP routing entries OSPF: OSPF routing entries ISIS: ISIS routing entires BGP: BGP routing entries TOTAL: All protocol entries.
IP routing table count	The number of the routing table
Global	Specifies the name of the current routing table. You can fill in this field with one of the following parameters: Global: VRF is disabled by default. VRF1: VRF name TOTAL: Summarization of all VRF routing tables.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 prefix-list

Use this command to view information about an IPv6 prefix list or entries in this list.

show ipv6 prefix-list [*prefix-name*]

Parameter Description

Parameter	Description
prefix-name	Name of the IPv6 prefix list

Defaults The configuration information about all IPv6 prefix lists is displayed by default.

Command Mode Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and route-map configuration mode.

Usage Guide If no prefix list is specified, the configurations of all prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Configuration Examples

```
Ruijie# show ipv6 prefix-list
Ipv6 prefix-list p6 : 2 entries
permit 13::/20
permit 14::/20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 route

Use this command to view information about an IPv6 routing table.

show ipv6 route [vrf *vrf-name*] [[*network* / *prefix-length*] | **summary** | *protocol*| **weight**]

Parameter Description

Parameter	Description
vrf-name	VRF name
network/prefix-length	(Optional) Only shows the route information to the target network.
summary	(Optional) Shows the classified statistics of the number of the ipv6 routes.
protocol	(Optional) Shows the routing protocol or the keyword connected or static. When specific protocol routes are displayed, use the keywords bgp, isis, ospf, and rip.
weight	(Optional) Only shows the non-default-weight routes.

Defaults All routes are displayed by default.

Command Mode Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and route-map configuration mode.

Usage Guide This command can be used to show specified route information flexibly based on specified options.

Configuration The following is the output of this command:

Examples

```
Ruijie(config)# show ipv6 route
IPv6 routing table -  Default - 7 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF external type 1, OE2
- OSPF external type 2
 ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
L     ::1/128  via Loopback, local host
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, VLAN 1
L     FE80::/10  via ::1, Null0
C     FE80::/64  via Loopback 1, directly connected
L   FE80::2D0:F8FF:FE22:33AB/128  via Loopback 1, local hostField
```

Field	Description
O	Source routing protocol, which may be: C: directly connected route L: Local host 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 route type 1 N2: OSPF NSSA external route type 2 IA: internal route in the OSPF routing area SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route ia: internal route in the IS-IS routing area
20::/64	Network address and mask of the target network
[1/0]	Management distance/metric value
Via 10::4	IPv6 address of the next hop
VLAN 1	Forwarding interface of the next hop

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.

Platform Description N/A

show key chain

Use this command to show the key chain configuration information in privileged user mode.

show key chain [*key-chain-name*]

Parameter Description

Parameter	Description
key-chain-name	(Optional) Only shows the configuration information about the specified key chain.

Defaults The configuration information about all key chains is displayed by default.

Command Mode Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and key chain configuration mode.

Usage Guide If no key chain is specified, the configuration information about all key chains is displayed, otherwise only the configuration of the specified key chain is displayed.

Configuration Examples

```
Ruijie# show 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	Name of the key chain
key	Key ID
text	Key string
accept-lifetime	Lifetime in the receiving direction
send-lifetime	Lifetime in the sending direction

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show route-map

Use this command to show the configuration information about a route-map in privileged user mode.

show route-map [*route-map-name*]

Parameter Description

Parameter	Description
route-map-name	(Optional) Only shows the configuration information about the specified route-map.

Defaults The configuration information about all route-maps is displayed by default.

Command Mode Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and route-map configuration mode.

Usage Guide If no route-map is specified, the configurations of all route-maps are displayed, otherwise only the configuration information about the specified route-map is displayed.

Configuration 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	Allows the route-map policy to contain the keyword permit.
sequence 10	Sequence number of the route-map policy.
Match clauses	Defines the match rule. Whether to perform the set operation depends on the keyword permit or deny in the route-map policy.
Set clauses	Sets the operation when the match rule is met.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

PBR Commands

ip local policy route-map

Command Function

Use this command to apply the policy-based routing (PBR) on the packets sent locally. Use the **no** form of this command to disable the function.

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

PBR is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

Configuration Examples

The following examples sends 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 host 192.168.217.10
```

The following example defines the route map:

```
Ruijie(config)#route-map lab1 permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set interface serial 2/0
Ruijie(config-route-map)#exit
```

The following example applies PBR on the local interface:

```
Ruijie(config)#ip local policy route-map lab1
```

Related

Command	Description

Commands

access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the output port of the policy-based routing .
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description

N/A

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 forwarding mode of policy-based routing.

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.


Caution 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 ACLs 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

ip policy route-map

Use this command to apply the policy-based routing on an interface. Use the **no** form of this command to disable the function.

ip policy route-map *route-map*

no ip policy route-map

Parameter Description

Parameter	Description
route-map	Name of the route map

Defaults

PBR 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.

Caution

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 host 10.0.0.1
Ruijie(config)#access-list 2 permit  host 20.0.0.1
```

The following example defines the route map:

```
Ruijie(config)#route-map lab1 permit 10
Ruijie (config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip next-hop 196.168.4.6
Ruijie(config-route-map)#exit
Ruijie(config)#route-map lab1 permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip next-hop 196.168.5.6
Ruijie(config-route-map)#exit
```

The following example applies the route map on the interface:

```
Ruijie(config)#interface FastEthernet 0/0
Ruijie(config-if)#ip policy route-map lab1
Ruijie(config-if)#exit
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.

set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the policy-based routing output port.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description N/A

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 disable the function.

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.
no	The packets sent locally are not controlld by the policy-based routing.

Defaults The local PBR 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 shows the PBR application process: The device sends the packets from the source address 2003:1000::10/80 to the 2001:100::/64, the packets will match ACL6 of aaa and be sent to the device 2003:1001::2:

The following example defines the ACL matched with the IPv6 packet:

```
Ruijie(config)#ipv6 access-list aaa
Ruijie(config)#permit ipv6 2003:1000::10/80 2001:100::/64
```

The following example defines the router map:

```
Ruijie(config)#route-map pbr-aaa permit 10
Ruijie(config-route-map)#match ipv6 address aaa
Ruijie(config-route-map)#set ipv6 next-hop 2003::1001::2
```

The following example applies the PBR on the device:

```
Ruijie(config)#ipv6 local policy route-map pbr-aaa
```

Related Commands

Command	Description
match ipv6 address	Sets the ACL6 used to match the IPv6 packets in the IPv6 PBR.
match length	Defines the length of matched packets.
route-map	Defines the route map for PBR.
set default interface	Defines the default next hop output port.
set interface	Defines the next hop output port.
set ipv6 default next-hop	Sets the default next hop of packet forwarding.
set ipv6 next-hop	Sets the next hop of packet forwarding.
set ipv6 precedence	Sets the priority field in the head of IPv6 packets.
show ipv6 policy	Shows the current PBR application.
show route-map	Shows the current router map configuration.

Platform Description N/A

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 forwarding mode of policy-based routing.

ipv6 policy {load-balance | redundance}

no ipv6 policy

Parameter Description

Parameter	Description
load-balance	Sets the policy as load balancing.
redundance	Sets the policy as redundant backup.

Defaults Redundant backup is adopted by default.

Command Mode Global configuration mode

Usage Guide This 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.

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 maps of the policy-based routing applied on the interface **FastEthernet** 0/0 takes effect.
The following example sets the ACLs.

```
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 the 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
```

The following example applies the policy-based routing on the interface.

```
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
Ruijie(config)# interface FastEthernet 0/0
Ruijie(config-if)# ipv6 policy route-map lab1
Ruijie(config-if)# exit
Ruijie(config)# ipv6 policy redundance
```

Related Commands

Command	Description
ipv6 policy route-map *route-map*	Applies PBR on a layer-3 interface.

Platform Description

N/A

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 disable the function.

ipv6 policy route-map *route-map*

no ipv6 policy route-map

Parameter Description

Parameter	Description
route-map	Route map name

Defaults

No PBR function is applied on interfaces 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.

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.

Router map rules applied by IPv6 PBR must be IPv6 supported rules, otherwise they will not take effect. When there are multiple router maps in the system, please make sure you apply the correct router map.

Configuration Examples

The following examples send the packets from network segment 10::/64to 2000: 1 and from network segment 20::/64 to 2000: 2 on interface fastEthernet 0/0:

The following example defines the ACL.

```
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 the 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 policy-based routing on 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
match ipv6 address	Sets the IPv6 ACL used to match the IPv6 packets in the IPv6 PBR.
route-map	Defines the route map.
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.

Platform Description N/A

show ip policy

Use this command to view the interface configured with the policy-based routing and the name of route map applied on the interface.

show ip policy

Parameter Description

Parameter	Description
N/A	N/A

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 shows 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

show ipv6 policy

Use this command to view which interfaces are configured with IPv6 PBR.

show ipv6 policy

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

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to show the interfaces applying IPv6 PBRs.
Configuration Examples	`N/A`

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

Platform Description	N/A

RIP Commands

auto-summary (RIP)

Use this command to enable automatic summary of RIP routes, and use the **no** form of this command to disable the 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.


Note

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

bdf all-interfaces (RIP)

Use this command to enable all interfaces running RIP to use the BDF for link detection, and use the **no** form of this command to restore to the default setting.

bdf all-interfaces

no bdf all-interfaces

Parameter Description

Parameter	Description
N/A	N/A

Defaults All interfaces running RIP are disabled 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

default-metric (RIP)

Use this command to define the default RIP metric value, and use the **no** form of this command to restore to the default configuration.

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
metric-value	Indicates the default metric value with the range of 1 to 16. If the metric value is greater than or equal to 16, the RGNOS regards the route unreachable.

Defaults The default value 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 shows that the RIP routing protocol redistributes 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

default-information originate (RIP)

Use this command to generate a default route in the RIP progress, and 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

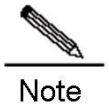
No default route is generated by default.
The default metric value is 1.

Command Mode

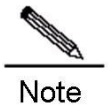
Routing prgrcess configuration mode

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.


Note

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.


Note

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 Commands

Command	Description
ip rip default-information	Notifies the default route through an interface.

redistribute	Redistributes the routes from other protocols to RIP.

Platform Description N/A

distance

Use this command to set the management distance of the RIP route, and use the **no** form of this command to restore to 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 of 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 value 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

distribute-list in (RIP)

Use this command to control route update for route filtering, and use the no form of this command to remove the configuration.

distribute-list {[*access-list-number* | *name*] | **prefix** *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*]} **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 shows that RIP controls 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

Parameter	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.

Platform Description

N/A

distribute-list out (RIP)

Use this command to control route update advertisement for filtering routes, and use the **no** form of this command to remove this definition.

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 shows that the RIP routing process 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

Parameter	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.
redistribute	Configures route redistribution.

Platform Description N/A

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 This command has no default behavior or default value.

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 shows how to enter or exit 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

graceful-restart (RIP)

Use this command to configure the RIP graceful restart (GR) function of a device. Use the **graceful-restart grace-period** command to display the grace period parameter used for configuring GR and enable the RIP GR function. You can use the **no** form of this command to restore to the default configuration.

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter Description

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	(Optional) Displays the configured grace-period.
grace-period	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The value is in the range of 1s to 1,800s.

Defaults GR is not enabled by default.

Command Mode Routing process configuration mode

Usage Guide

The GR function is configured on the basis of RIP instances. Different parameters can be configured for different RIP instances.

The GR period is the longest time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation.

The **graceful-restart grace-period** command allows you to display the modified GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If the value is incorrectly configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, you are advised not to adjust the GR period. If the period needs to changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the **timers basic** command.


Caution During the RIP GR period, the network must be stable.

Configuration Examples The following example enables the RIP GR function and configures the GR period parameters of the GR function.

```
Ruijie(config)# router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

Related Commands

Command	Description
timers basic	Configures RIP timers.

Platform Description N/A

ip rip authentication key-chain

Use this command to enable RIP authentication and specify the keychain used for RIP authentication, and use the **no** form of this command to delete the specified keychain.

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 verion of RIP packets sent on the interface.
key chain	Defines the keychain and enters keychain configuration mode.

Platform Description N/A

ip rip authentication mode

Use this command to define the RIP authentication mode, and use the no form of this command to restore to the default RIP authentication mode.

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

Command	Description

Commands		
	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

ip rip authentication text-password

Use this command to enable RIP authenticatoin and set the password string of RIP plaintext authentication, and use the **no** form of this command to remove the password string.

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 ciphertext.
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

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, and use the **no** form of this command to remove the configuration on the interface..

ip rip bfd [**disable**]

no ip rip bfd [**disable**]

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 enanble 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

ip rip default-information

Use this command to advertise the default route through a RIP interface, and use the **no** form of this command to cancel the notification of the default route.

ip rip default-information {**only** | **originate**} [**metric** *metric-value*]

no ip rip default-information

Parameter Description

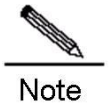
Parameter	Description
only	Notifies the default route rather than other routes.
originate	Notifies the default route and other routes.
metric *metric-value*	Specifies the metric value of the default route, in the range of 1-15.

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

ip rip receive enable

Use this command to enable RIP to receive the RIP data package on a specified interface, and use the **no** form of this command to prohibit receiving the RIP data package on the interface.

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 Commands

Parameter	Description
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

ip rip receive version

Use this command to define the version of RIP packets received on an interface, and use the **no** form of this command to restore to the default value.

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

ip rip send enable

Use this command to enable RIP to send a RIP data package on a specified interface, and use the **no** form of this command to disable sending the RIP data package on the interface.

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

Parameter	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

ip rip send supernet-routes

Use this command to enable RIP to send the supernet route on a specified interface, and use the **no** form of this command to disables sending the RIP supernet route on the specified interface.

ip rip send supernet-routes

no ip rip send supernet-routes

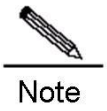
Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP supernet routes can be sent through the interface 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

ip rip send version

Use this command to define the version of the RIP packets sent on the interface, and use the **no** form of this command to restore to the default value.

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

ip rip split-horizon (RIP)

Use this command to enable split horizon, and use the **no** form of this command to disable the 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 Split horizon with no poisoned reverse 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

Command	Description

commands		
	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

ip rip summary-address

Use this command to configure port-level convergence through an interface, and use the **no** form of this command to disable convergence of the specified IP address or subnet.

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.


Note

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

Parameter	Description
auto-summary	Enables the automatic convergence of RIP routes.

Platform Description

N/A

ip rip triggered

Use this command to enable triggered RIP based on links, and use the **no** form of this command to disable triggered RIP.

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 value ranges from 1s to 3600s, and 5s is the default value.
retransmit-count *count*	Configures the maximum times that the Update Request and Update Response packets are retransmitted. The value ranges from 1 to 3600, and 36 is the default value.

Defaults

TRIP is not enabled 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 specifies the retransmission interval and maximum retransmission time as 10s 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

Parameter	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

ip rip v2-broadcast

Use this command to send RIPv2 pakcets in broadcast rather than multicast mode, and use the **no** form of this command to restores to 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

Parameter	Description
version	Defines the default version of the RIP packets received and sent on the interface.

Platform Description N/A

network (RIP)

Use this command to define the list of networks to be advertised in the RIP routing process, and 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 Routing process configuration mode

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

neighbor (RIP)

Use this command to define the IP address of a RIP neighbor, and use the **no** form of this command to delete the neighbor definition.

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 shows used commands and defines that RIP advertises route information to only neighbor 192.168.1.2.

```
Ruijie (config)# router rip
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# neighbor 192.168.1.2
```

Related Commands

Command	Description
passive-interface	Configures the interface as a passive interface.

Platform Description

N/A

offset-list (RIP)

Use this command to increase the metric value of received or sent RIP routes, and use the **no** form of this command to delete the specified offset list.

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 ranges from 0 – 16.
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

output-delay

Use this command to modify the delay to send RIP update packets, and use the **no** form of this command to remove the configuration.

output-delay *delay*

no output-delay

Parameter Description

Parameter	Description
delay	Sets the delay to send RIP update packets in the range from 8 ms to 50 ms.

Defaults No sending delay is configured by default.

Command Mode Routing process configuration mode

Usage Guide

In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible.

However, when a high-speed device sends a large number of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Configuration 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

passive-interface

Use this command to disable the function of sending update packets on an interface, and use the no form of this command to re-enable this function.

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

redistribute (RIP)

Use this command to redistribute external routes in route configuration mode, and use the **no** form of this command to cancel the configuration.

redistribute {**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static**} [{**level-1 | level-1-2 | level-2**}] [**match** {**internal | external** [**1**|**2**] | **nssa-external** [**1**|**2**]}] [**metric** *metric-value*] [**route-map** *route-map-name*]

no redistribute {**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static**} [{**level-1 | level-1-2 | level-2**}] [**match** {**internal | external** [**1**|**2**] | **nssa-external** [**1**|**2**]}] [**metric** *metric-value*] [**route-map** *route-map-name*]

Parameter Description

Parameter	Description
bgp	Is redistributed from bgp.
connected	Is redistributed from a connected route.
isis *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 ranges 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 ranges 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

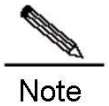
This command is executed to redistribute external routes to RIP.

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.



Note

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

Caution

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

router rip

Use this command to create the RIP routing process and enter the routing process configuration mode, and use the **no** form of this command to delete the RIP routing process.

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 describes how to create the RIP routing process and enter 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

timers basic

Use this command to adjust the RIP clock, and use the **no** form of this command to restore to the default configuration.

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 180s.
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 s.

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 30s, 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

Command	Description

Commands	N/A	N/A

Platform Description N/A

validate-update-source

Use this command to validate the source address of the received RIP route update packet, and use the **no** form of the command to disable source address validation.

validate-update-source

no validate-update-source

Parameter Description

Parameter	Description
N/A	N/A

Defaults Verification of the source IP address of update packets 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

version (RIP)

Use this command to define the RIP version of a device, and use the no form of this command to restore to the default configuration.

version {**1** | **2**}

no version

Parameter Description

Parameter	Description
1	Defines the RIP version 1.
2	Defines the RIP version 2.

Defaults

The route update packets of RIPv1 and are received by default, but only the RIPv1 route update packets are sent.

Command Mode

Routing process configuration mode

Usage Guide

This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

Configuration 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

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, or 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 shows 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

show ip rip database

Parameter Description

Use this command to show the route summary information in the RIP routing database.

show ip rip database [**vrf** *vrf-name*] [*network-number network-mask*] [**count**]

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, or 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 shows 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 shows 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 shows 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	Shows the information of the currently-running routing protocol process.

Platform Description N/A

show ip rip external

Use this command to show the information of the external routes redistributed by the RIP protocol.

show ip rip external [**bgp** | **connected** | **isis** [*process-name*] |**ospf** <*1-65535*>| **static**] [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
bgp | connected | isis | ospf | static	Shows the external route redistributed by the specified routing protocol (optional).
vrf *vrf-name*	Shows the RIP external route of the specified VRF (optional).
process-name	Specifies the ISIS instance name.
<1-65535>	Specifies the ID of the OSPF instace.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, or routing process configuration mode

Usage Guide N/A

Configuration Examples

The following examples the 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	Shows the information of the currently running routing protocol process.

Platform Description

N/A

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*	Shows the RIP interface of specified VRF (optional).
[*interface-type interface-number*]	Shows the specified interface type and interface number (optional).

Defaults

N/A

Command Mode

Privileged EXEC mode, global configuration mode, or 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 examples the RIP interface information.

```
Ruijie# show ip rip interface
FastEthernet 01 is down, line protocol is down
  RIP is not enabled on this interface
FastEthernet 1/0 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv2 packets only
    Send RIPv2 packets only
    Passive interface: Disabled
    Split horizon: Enabled
    V2 Broadcast: Disabled
    Multicast register: 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
```

If the BFD has been configured for RIP, the BFD information is also shown:

```
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 supernet routes: Enabled
   Passive interface: Disabled
   Split horizon: Enabled
   V2 Broadcast: Disabled
   Multicast registe: Registed
   Interface Summary Rip:
     Not Configured
 IP interface address: 2.2.2.111/24
```

Related Commands

Command	Description
show ip rip	Shows the information of the currently running routing protocol process.

Platform Description N/A

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) Shows the IP address of a specified RIP neighbor.
vrf *vrf-name*	(Optional) Shows the RIP interface of a specified VRF.

Defaults N/A

Command Privileged EXEC mode, global configuration mode, or routing process configuration mode

Mode

Usage Guide

This command is used to show the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.

Configuration Examples

The following example shows 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	Shows the information of the routing protocol process that is running.

Platform Description

N/A

OSPFv2 Commands

area

Use this command to configure the specified OSPF area. Use the **no** form of this command to remove the specified OSPF area.

area *area-id*

no area *area-id*

Parameter Description

Parameter	Description
area-id	IDof 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 anarea 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

area authentication

Use this command to enable OSPF area authentication in routing process configuration mode. Use the **no** form of this command to disable OSPF area authentication.

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) EnablesMD5 (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 fastEthernet0/1
Ruijie(config-if-FastEthernet 0/1)# ip address192.168.12.1
255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key1md5 backbone
#Configure OSPF routing protocol.
Ruijie(config)# router ospf 1
Ruijie(config-router)# network192.168.12.0
0.0.0.255 area 0
Ruijie(config-router)# area0 authentication
message-digest
```

Related

Command	Description

Commands		
	ip ospfauthentication-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

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 value.

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 1 to 16777214.

Defaults The default value 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 Description N/A

area filter-list

Use this command to filter the inter-area routes on the ABR.

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
access | **prefix**	Associated prefix list or ACL
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

Commands	Description
N/A	N/A

Platform Description

N/A

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**<*1-2*>]] [**no-summary] [translator [stability-interval** *seconds* | **always**]]

no area *area-id* **nssa [no-redistribution][default-information-originate[metric** *value*]**[metric-type** <*1-2*>**]] [no-summary] [translator [stability-interval| always]]**

Parameter Description

Parameter	Description
area-id	NSSAID
no-redistribution	(Optional) Imports the routing information to a common area other than the NSSA for the NSSAABR.
default-information originate	(Optional) Generates and imports the default Type 7 LSA to the NSSA. This option takes effect only on the NSSA ABR or ASBR.
Metric value	(Optional) Sets the metric of the generated default LSA. The range is from 0 to 16777214. The default value is 1.
metric-type<1-2>	(Optional) Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
no-summary	(Optional) Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
translator	(Optional) 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.

Note

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

area range

Use this command to configure inter-area route aggregation for OSPF in routing process configuration mode. Use the **no** form of this command to delete route aggregation. Use the no form with the cost parameter to restore the default metric of the aggregate route, but not delete route aggregation.

area *area-id* **range** *ip-address net-mask* **[advertise | not-advertise] [cost** *cost***]**

no area *area-id* **range** *ip-address net-mask* **[cost]**

Parameter Description

Parameter	Description
area-id	ID of the area where the aggreate 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 aggreagate 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 Mode

Routing process configuration 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 aggregates 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

Commands	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

area stub

Use this command to set an OSPF area as a stub area or full stub area in routing process configuration mode. Use the **no** form of this command to delete the configuration of the stub area or full stub area.

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 N/A

Description

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 delete the virtual link.

area *area-id* **virtual-link** *router-id* **[authentication [message-digest | null]] [dead-interval** *{seconds***| minimal hello-multiplier** *multiplier}***] [hello-interval** *seconds]* **[retransmit-interval** *seconds]* **[transmit-delay** *seconds***] [[authentication-key[0|7]***key***] | [message-digest-key** *key-id* **md5[0|7]***key***]]**

no area *area-id* **virtual-link** *router-id* **[authentication] [dead-interval] [hello-interval] [retransmit-interval] [transmit-delay] [[authentication-key] | [message-digest-key** *key-id]]*

Parameter 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.
minimal	Enables the Fast Hello function and sets the death clock to 1 second.
hello-multiplier	Multiplies dead-interval with hello-interval in the Fast-Hello function.
multiplier	Specifies the number of Hello packets that are sent every second in the Fast Hello function. The range is from 3 to 20.
hello-interval *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 ciphertext.

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 ciphertext.
authentication	Sets the authentication type to plain text.
message-digest	Sets the authentication type to MD5.
null	Sets the authentication type to no authentication.

Defaults

The following are the default values:
dead-interval: 40seconds
hello-interval: 10seconds
retransmit-interval: 5seconds
transmit-delay: 1second
authentication: null
The Fast Hello function is disabled by default.
The other parameters do not have default values.

Command Mode

Routing process configuration mode

Usage Guide

A virtual link can connect an area to the backbone area, or another non-backbone area. In the OSPF routing domain, all areas must connect to the backbone area. If an area disconnects from the backbone area, avirtual 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 shown 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 linkin routing process configuration mode.
OSPF supports the Fast Hello function.
If the Fast Hello function is enabled, the OSPF can discover neighbors and detects invalid neighbors quickly. You can enable the OSPF Fast Hello function by specifying the keywords minimal and hello-multiplier, and the multiplier parameter. You can set the death clock to 1 second in minimal and hello-multiplier to a value equal to or greater than 2. In this case, the Hello packet sending interval is less than 1 second.
The hello-interval field of a Hello packet received by a virtual link is omitted if the Fast Hello function is enabled on the virtual link and the hello-interval field is set to 0 for Hello packets advertised from the virtual link.
No matter the Fast Hello function is enabled or not, the values of dead-interval must be consistent on both ends of a virtual link. The values of hello-multiplier on both ends can be different if at least one Hello packet can be received within dead-interval. You can use the show ip ospf virtual-links command to monitor dead-interval and hello-interval configured for a virtual link.

Caution For the Fast Hello function, you can only configure either the **dead-interval minimal hello-multiplier** parameter or the **hello-interval** parameter.

Configuration Examples

Example 1 sets area 1 as the transition area to establish virtual link with neighbor *2.2.2.2.*

```
Ruijie(config)# routerospf 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
Example 2 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 packetauthentication 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
Example 3 sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1, enables the Fast Hello function on this virtual link, and sets the multiplier to 3.
Ruijie(config)# routerospf1
Ruijie(config-router)# network172.16.17.0 0.0.15.255 area1
Ruijie(config-router)# network 172.16.252.0 0.0.0.255 area10
Ruijie(config-router)#  area1  virtual-link1.1.1.1dead-interval  minimal hello-multiplier 3
```

Related Commands

Command	Description
area authentication	Enables the OSPF area packet authentication and define the authentication mode.
show ip ospf	Shows the OSPF process information, including the router ID.
show ip ospf virtual-links	Monitors information about a virtual link.

Platform Description

N/A

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 disable this function and restores the default value.

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.

Default The reference bandwidth is 100Mbps by default.

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 10Mbps.

```
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	Shows the OSPF global configuration information

Platform Description N/A

bdf all-interfaces(OSPF)

Use this command to enable Bidirectional Forwarding Detection (BFD) on all OSPF interfaces. Use the no form of this command to restore the default configuration.

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 thebfd all-interfaces command in routing process configuration mode.

Configuration Examples

N/A

Related Commands

Command	Description
router ospf process-id [**vrf** *vrf-name*]	Creates the OSPF routing process and entersrouting process configuration mode.
ip ospf bfd [**disable**]	Enables or disables the BFD on the specified OSPF interface.

Platform Description

N/A

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 specifiedinstanceand 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 1583is 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

Commands	Description
N/A	N/A

Platform Description N/A

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).

commpatible rfc1583

no commpatible rfc1583

Parameter Description

Parameter	Description
N/A	N/A

Defaults The RFC 1583rule is used by default.

Command Routing process configuration mode

Mode

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	Shows the OSPF global configuration information

Platform Description

N/A

default-information originate (OSPF)

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 disable the default route.

default-information originate [always] [metric *metric***] [metric-type** *type***] [route-map** *map-name***]**

no default-information originate [always] [metric metric]

[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 routein 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 show the

default route. To make sure whether the default route is generated, use the **show ip ospf database** command to show 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 shows only the type 1 route.

The routers in the stub area cannot generate external default routes.


Caution

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 exampleconfigures that OSPF generates an external default route and injects it to the OSPF routing domain. The default route is of type 1 and the metric50.

```
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	Shows OSPF link state database.
show ip route	Shows the IP route table.
redistribute	Redistributes routes of other routing processes.

Platform Description

N/A

default-metric

Use this command to set the **default metric** of OSPF redistribution route in routing process mode. Use the **no** form of this command to restore the default configuration.

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	Shows the OSPF global configuration information.

Platform Description	N/A

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

distance ospf

Use this command to set the Administration Distance (AD) of different types of OSPF routes.

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 ADto 160.

```
Ruijie(config)# routerospf1
Ruijie(config-router)# distance ospf external 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

distribute-list in

Use this command to configure LSA filtering.

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

```
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

distribute-list out

Use this command to configure filtering redistribution routes. The function is similar to that of the **redistribute** command.

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

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 configuration.

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults The MIB is bound with the OSPFv2 process withthe 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 overSimple 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	Shows the OSPF global configuration information.
enable traps	Configures the OSPF TRAP function.

Platform Description N/A

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 disable sending the specified TRAP messages.

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

Parameter	Description
error	Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches. **Ifauthfailure** Interface authentication error **Ifconfigerror** Interface parameter configuration error **Ifrxbadpacket** Error packets received on the interface **Virtifauthfailure** Authentication error on the virtual interface **Virtifconfigerror** Parameter configuration error on the virtual interface **Virtifrxbadpacket** Error packets received on the virtual interface
isa	Configures all traps switches related to the LSA. Use this parameter to set the following specified LSAtraps switches. **Lsdbapproachoverflow** External LSA count has reached the 90% of the upper limit. **Lsdboverflow** External LSA count has reached the upper limit. **Maxagelsa** LSA reaching the aging time **Originatelsa** Generates new LSA
retransmit	Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches. **Iftxretransmit** Packet retransmission on the interface **Virtiftxretransmit** Packet retransmission on the virtual interface

state-change	Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches.	
	Ifstatechange	Interface state change
	NbrRestartHelper StatusChange	State change during the neighbor GR process
	Nbrstatechange	Neighbor state change
	NssaTranslatorStatusChange	State change of the NSSA translator
	RestartStatusChange	State change of the GR Restarter on the device
	Virtifstatechange	State change on the virtual interface
	VirtNbrRestartHelper StatusChange	Status change of the virtual neighbor GR process
	Virtnbrstatechange	State change on the virtual neighbor

Defaults All TRAP switches are disabled by default.

Command Mode Routing process configuration mode

Usage Guide The snmp-server enable traps ospf command must be configured before you configure this command, for it is limited by the snmp-server command.
This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Configuration 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	Shows 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

graceful-restart

Use this command to configure 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 restore the default configuration..

graceful-restart [graceful-period *grace-period***]**

no graceful-restart [graceful-period]

Parameter Description

Parameter	Description
grace-period	(optional)Explicitly configuresgrace-period.
grace-period	User-set GR intervalin the range from1 to 1800 seconds. It is the longest time between the OSPF invalidation and the OSPF graceful restart.

Defaults GR is disabled by default. The default value of grace-period is 120 seconds.

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.


Caution GR is unavailable when the Fast Hello function is enabled.

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

graceful-restart helper

Use this command to enable the graceful restart helper function. Use the **no** form of this command to restore the default configuration.

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

Command	Description

Commands		
	gracful-restart	Enables GR on the device.

Platform Description N/A

ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of the command to restore the default type.

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 onfastEthernet 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

ip ospf authentication-key

Use this comand to configure the OSPF plain text authentication key in interface configuration mode. Use the **no** form of this command to delete the plain text authentication key.

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 ciphertext.
key	Key containingat 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

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 remove the setting on the interface.

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 *process-id* [**vrf** *vrf-name*]	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

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 configuration.

ip ospf cost *cost*

no ip ospf cost

Parameter Description

Parameter	Description
cost	OSPF interface cost in the range from0 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	Specifiesthe interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Shows the OSPF global configuration information

Platform Description

N/A

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 configuration.

ip ospf database-filter all out

no ipospf 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 examplestops 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

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 **ip ospf dead-interval** minimal hello-multiplier command in interface configuration mode to enable the Fast Hello function of OSPF. Use the **no** form of this command to restore the default configuration.

ip ospf dead-interval {*seconds* **| minimal hello-multiplier** *multiplier***}**

no ip ospf dead-interval

Parameter Description

Parameter	Description
seconds	Defines the interval for determining the neighbor death in seconds. The range is from0 to 2147483647.
minimal	Enables the Fast Hello function and sets the death clock to 1 second.
hello-multiplier	Multiplies dead-interval with hello-interval in the Fast-Hello function.
multiplier	Specifies the number of Hello packets that are sent every second in the Fast Hello function. The range is from 3 to 20.

Defaults

The value of dead-interval is 4 times the interval configured with the ip ospf hello-interval command by default.
The Fast Hello function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

The OSPF dead-interval is included in the Hello message. If the OSPF does not receive the Hello packets from its neighbor within the dead-interval, it declares the neighbor's death and deletes its entry in the neighbor list. The value of dead-interval is 4 times the hello-interval. The modification of hello-interval will automatically change the dead-interval.
This command can be used to manually change the value of dead-interval. Note that:

- The value of dead-interval cannot be less than the interval of Hello messages.
- The values of dead-interval for all devices in the same network segment must be the same.

OSPF supports the Fast Hello function.
If the Fast Hello function is enabled, the OSPF can discover neighbors and detects invalid neighbors quickly. You can enable the OSPF Fast Hello function by specifying **minimal, hello-multiplier**, and *multiplier*. You can set the death clock to 1 (unit: second) in **minimal** and **hello-multiplier** to a value equal to or greater than 2. In this case, the Hello packet sending interval is less than 1 second.
The Hello interval field of a Hello packet received by an interface is omitted, if the Fast Hello function is enabled on the interface and the hello-interval field is set to 0 for Hello packets advertised from the interface. No matter the Fast Hello function is enabled or not, the dead-intervals must be consistent on a same network segment. The values of **hello-multiplier** on a same network segment can be different if at least one Hello packet can be received within the dead-interval. You can use the **show ip ospf interface** command to monitor dead-interval and hello-interval configured for an interface.


Caution For the Fast Hello function, **dead-interval minimal hello-multiplier** and **hello-interval** cannot be configured at the same time.

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
The following example enables the Fast Hello function on fastEthernet 0/1 and
configures hello-multiplierto 3.
```

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf dead-interval minimal
hello-multiplier 3
```

Related Commands

Command	Description
ip ospf hello-interval	Specifies the interval at which the OSPF sends Hello packets
show ip ospf interface	Monitors OSPF interface information.

Platform Description N/A

ip ospf disable all

Use this command to prevent the specified interface from generating OSPF packets.

ip ospf disable all

no ipospf disable all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

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

```
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

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 configuration.

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 Examples

The following example configures the interval of sending the Hello packets on fastEthernet 0/1 to15.

```
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

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 delete the MD5 authentication key.

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

Command	Description

Commands		
	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

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 configuration.

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

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 configuration.

ip ospf source-check-ignore

no ip ospf source-check-ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults The source address check in the point-to-point link 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

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 configuration.

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 thedesignated 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

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 configuration.

ip ospf priority *priority*

no ip ospf priority

Parameter Description

Parameter	Description
priority	Sets the OSPF priority of the interface in the range from0 to 255.

Defaults The default priority 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

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 configuration.

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 from0 to 65535. This interval must be greater than the round trip delay of packets between two neighbors.

Defaults The default value is 5 seconds.

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

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 configuration.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter

Parameter	Description

Description	*seconds*	LSU packet transmission delay in seconds in the range from0 to 65535.

Defaults The default value is 1 second.

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

log-adj-changes

Use this command to enable the logging of the neighbor state changes. Use the no or default 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	Shows the OSPF global configuration information.

Platform Description

N/A

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.

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 value 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 setsthe maximum number of DD packets as 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

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 cancel the maximum metric.

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.

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 server 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.

Note

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 exampleconfiguresthe 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	Shows the OSPF related configurations.

Platform Description

N/A

neighbor

Use this command to define the OSPF neighbor in routing process configuration mode. Use the **no** form of this command to delete the specified neighbor.

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 from0 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 from0 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 from0 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

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 delete the OSPF area definition of the interface.

Network *ip-address wildcard* **area** *area-id*

no network *ip-address wildcard* **area** *area-id*

Parameter

Parameter	Description

Description

ip addres	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 assgined 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

overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance.

overflow database<*1-4294967294*> **[hard | soft]**

no overflow database

Parameter Description

Parameter	Description
<1-4294967294>	Maximum number of LSAs
hard | soft	hard: shuts down the OSPF instance when the number of LSAs exceeds that number. soft: issues an alarm when the number of LSAs exceeds that number.

Defaults

The maximum number of LSAs supported by the current OSPF instance is not restricted by default.

Command Mode

Routing process configuration mode

Usage Guide

To shut down the OSPF instance when the number of LSAs exceeds that number, use the hard parameter; otherwise, use the soft parameter.

Configuration Examples

The following example configures that OSPF instance 10 will be shut down when there are more than 10 LSAs.

```
Ruijie# config 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

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.

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 from0 to 2147483647.
wait-time	Waiting time of the routing device from the overflow status to normal status. The range is from0 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 can not 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

Command	Description

Commands	N/A	N/A

Platform Description N/A

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 disabe this function.

overflow memory-lack

no overflow memory-lack

Parameter Description

Parameter	Description
N/A	N/A

Defaults OSPF is allowed to enter the OVERFLOW state when the memory is insufficient 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	Shows the OSPF information.

Platform Description N/A

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 configuration.

passive-interface {default | *interface-type interface-number*}

no passive-interface {default | *interface-type interface-number*}

Parameter Description

Parameter	Description
interface-type interface-number	Interface to be set as a passive interface
default	Sets all the interfaces as passive interfaces

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.

Configuration Examples

The following example configures fastEthernet 0/1 as a passive interface.

```
Ruijie(config)# routerospf 30
Ruijie(config-router)# passive-interface fastEthernet 0/1
```

Related Commands

Command	Description
show ip ospf interface	Shows the configuration information of the interface.

Platform Description

N/A

redistribute

Use this command to redistribute the external routing information.

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 isis instance specified in area-tag
Ospf *process-id*	Redistribution from an ospf instance specified in process-idin the range from 1 to 65535
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 from0 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.


Caution

The range of set metricis 0 to 16777214 for the associated route-map. If the value exceeds the range, introducing a route fails.


Note

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

Example 1 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 is 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

router ospf

Use this command to create the OSPF routing process in global configuration mode. Use the **no** form of this command to delete the defined OSPF routing process.

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 Based on the original implementation, the RGOS10.1 adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.

Configuration Examples The following example creates the OSPF routing process 10 within the specified vrf: vpn_1.

```
Ruijie(config)# router ospf10 vrf: vpn_1
```

Related Commands

Command	Description
show ip protocols	Shows the routing protocol informatin.
show ip ospf	Shows the OSPF information.

Platform Description	N/A

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.

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 value 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 as 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

router-id

Use this command to set the router ID. Use the **no** form of this command to delete the setting or restore the default configuration.

router-id *router-id*

no router-id

Parameter

Parameter	Description

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	Shows the routing protocol information.

Platform Description

N/A

summary-address

Use this command to configure the aggregate route out of the OSPF routing domain in routing process configuration mode. Use the **no** form of this command to delete the aggregate route.

summary-address *ip-address net-mask* **[not-advertise | tag** *value***]**

no summary-address *ip-address net-mask* **[not-advertise | tag** *value***]**

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 4294967295.

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

timers lsa arrival

Use this command to configure the time delay for the same LSA recieved. Use the **no** form of the command to restore the default configuration.

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 is0 to 600000.

Defaults 1000 milliseconds

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	Shows the OSPF information.

Platform Description N/A

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 the command to restore the default configuration.

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 to1800seconds.

Defaults 240 seconds

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 followingexample configures the pacing time as 120seconds.
	`Ruijie(config)# deviceospf 20`
	`Ruijie (config-router)# timers paing lsa-group 120`

Related Commands	**Command**	**Description**
	show ip ospf	Shows the OSPF information.

Platform Description	N/A

timers pacing lsa-transmit

Use this command to transmit the LSA grouping updating. Use the **no** form of the command to restore the default value.

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 10 to 1000.
	transmit-count	Configures the number of LS-UPD packets per group. The range is 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	Shows the OSPF process information, including the router ID.

Platform Description

N/A

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 in routing process configuration mode. Use the **no** form of this command to restore the default configuration.

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 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 is0 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: 10seconds.
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	Shows 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

timers throttle lsa all

Use this command to configure the exponential back off algorithmin for the LSA in routing process configuration mode. Use the **no** form of this command to restore the default configuration.

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 is1 to 600000.
hold-time	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is1 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.

Caution The value of hold-time cannot be smaller than that of delay-time, and the 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	Shows the configuration information of the ospf

Platform Description

N/A

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 configuration.

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 milli-secondsin the range from1 to 600000. 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 600000.
spf-max-waittime	Defines the maximum interval between two SPF calculations, in milliseconds in the range from1 to 600000.

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 untill 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 flexiblely 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.

Note

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 ofspf-delay;

The value of spf-max-waitime cannot be smaller than the value of spf-holdtime, or the value ofspf-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 thetimers 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 intervalsare: 5ms, 1second, 3 seconds, 7 seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90seconds…

```
Ruijie(config)# routerospf20
Ruijie(config-router)# timers throttle spf 5 1000 90000
```

Related Commands

Command	Description
show ip ospf	Shows the configuration information of OSPF
timers spf	Configures the SPF calculation delay. This command is supported in versions earlier than RGOS 10.4. It is recommended to replace the timers spf command with the timers throttle spf command.

Platform Description

N/A

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	Shows the configuration information of the OSPF

Platform Description N/A

show ip ospf

Use this command to show the OSPF information in privileged user mode.

show ip ospf [*process-id*]

Parameter Description	Parameter	Description
	process-id	OSPF process ID

Defaults N/A

Command Mode Privileged user mode

Usage Guide This command shows the information of the OSPF routing process.

Configuration Examples The following is 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 whendevice-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	Supportsopaque-LSA.
Graceful-restart	GR Restart capability described in the RFC3623 Graceful Restart
Graceful-restart helper	GR Help capability described in the RFC3623 Graceful Restart
Router Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	Parameter used for LSA pacing, checksum calculation, and aging interval
Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.

Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this router	Total number of areas on the devices
Area type	Area type, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSATranslatorState	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA.

BFD enabled	Enables BFD for OSPF.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip ospf border-routers

Use this command to show the OSPF internal routing table on the ABR/ASBR in privileged user mode.

show ip ospf [*process-id***] border-mrouters**

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged user mode

Usage Guide This command shows 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 is 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	Shows the OSPF ID of the border device.
[2]	Shows the cost to the border device.
via 10.0.0.1	Shows the next-hop gateway to the border device.
FastEthernet 0/1	Shows the interface to the border device.
ABR, ASBR	Shows the type of the border device, including ABR, ASBR, or both.
Area 0.0.0.1	Shows 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

show ip ospf database

Use this command to show the OSPF link state database information in privileged user mode.

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]**

Parameter Description

Parameter	Description
area-id	(Optional) Shows the area ID.
adv-device	(Optional) Shows the LSA information generated by the specified advertising device.
link-state-id	(Optional) Shows the LSA information of the specified OSPF link state identifier.
self-originate	(Optional) Shows the LSA information generated by the device itself.
Max-age	(Optional) Shows the LSAs aged.
router	(Optional) Shows the OSPF device LSA information.
network	(Optional) Shows the OSPF network LSA information.
summary	(Optional) Shows the OSPF summary LSA information.
asbr-summary	(Optional) Shows the ASBR summary LSA information.
external	(Optional) Shows the OSPF external LSA information.
nssa-external	(Optional) Shows the category 7 OSPF external LSA information.
opaque-area	(Optional) Shows type 10 LSAs.
opaque-as	(Optional) Shows type 11 LSAs.
opaque-link	(Optional) Shows type 9 LSAs.
database-summary	(Optional) Shows the statistics of LSAs of the link state database.

Defaults N/A

Command Mode Privileged user mode

Usage Guide When the OSPF link state database is very large, you should show the information on the link state database by item. Proper use of commands may help OSPF troubleshooting.

Configuration Examples

The following is 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 thefields in the output of the show ip ospf database command.

Field	Description
OSPF Device with ID	Shows the Router ID.
Device Link States	Shows the device LSA information.
Net Link States	Shows the network LSA information.
Summary Net Link States	Shows the summary network LSA information.
NSSA-external Link States	Shows the type 7 autonomous external LSA information.
AS External Link States	Shows the type 5 autonomous external LSA information.
Link ID	Shows the Link ID.
ADV Device	Shows the ID of the device that advertises the LSAs.
Age	Shows the keepalive period of the LSA.

Seq#	Shows the sequentce number of the LSA, which is used to check aged or duplicate LSAs.
Cksum	Shows the checksum of LSAs.
Link-Count	Shows the number of links in the device LSA information.
Route	Shows the device information included in the LSA.
Tag	Shows the tag of the LSA.

The following is 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	Shows the router ID.
AS Summary Link States	Shows the summary LSA information in the AS.
LS age	Shows the keepalive period of the LSA.
Options	Option
LS Type	Shows the type of the LSA.
Link State ID	Shows the link ID of the LSA.
AdvertisingRouter	Shows the device advertising the LSA.
LS Seq Number	Shows the sequentce number of the LSA.
Checksum	Shows the checksum of the LSAs.
Length	Shows the length (in bytes) of the LSA.
Network Mask	Shows the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be only 0 now.
Metric	Shows the metric of the route corresponding to the LSA.

The following is 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	Shows the router ID.
Type-5 AS External Link States	Shows autonomous external LSA information.
LS age	Shows the keepalive period of the LSA.
Options	Option
LS Type	Shows the type of the LSA.
Link State ID	Shows the link ID of the LSA.
Advertising Router	Shows the device advertising the LSA
LS Seq Number	Shows the sequentce number of the LSA.
Checksum	Shows the checksum of the LSAs.
Length	Shows the length (in bytes) of the LSA.
Network Mask	Shows 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	Shows 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 processestoredistributeOSPF routes.

The following is 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	Shows the router ID corresponding to the follow-up information and the process ID corresponding to the OSPF.
Network LinStates	Shows the network LSA information.
LS age	Shows the keepalive period of the LSA.
Options	Option
LS Type	Shows the type of the LSA.
Link State ID	Shows the link ID of the LSA.
Advertising Device	Shows the device advertising the LSA.
LS Seq Number	Shows the sequentce number of the LSA.
Checksum	Shows the checksum of LSAs.
Length	Shows the length (in bytes) of the LSA.
Network Mask	Shows the network mask of the network corresponding to the LSA.
Attached Router	Shows the device that is connected with the network.

The following is 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	Shows the router ID.
Device Link States	Shows the device LSA information.
LS age	Shows the keepalive period of the LSA.
Options	Option
Flag	Flag
LS Type	Shows the type of the LSA.
Link State ID	Shows the link ID of the LSA.
Advertising Router	Shows the device advertising the LSA.
LS Seq Number	Shows the sequence number of the LSA.
Checksum	Shows the checksum of LSAs.
Length	Shows the length (in bytes) of the LSA.
Number of Links	Shows the number of links associated with the device.
Link connected to	Shows 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 is 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	Shows the router ID.
Summary Net Link States	Shows the summary network LSA information.
LS age	Shows the keepalive period of the LSA.
Options	Option
LS Type	Shows the type of the LSA.
Link State ID	Shows the link ID of the LSA.
Advertising Router	Shows the device advertising the LSA.
LS Seq Number	Shows the sequence number of the LSA.
Checksum	Shows the checksum of LSAs.
Length	Shows the length (in bytes) of the LSA.
Network Mask	Shows the network mask of the route corresponding to the LSA.
TOS	TOS value, supporting only 0 now
Metric	Shows the metric of the route corresponding to the LSA.

The following is 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	Shows the router ID.
NSSA-external Link States	Shows the type 7 autonomous external LSA information.
LS age	Shows the keepalive period of the LSA.
Options	Option
LS Type	Shows the type of the LSA.
Link State ID	Shows the link ID of the LSA.
Advertising Router	Shows the device advertising the LSA.
LS Seq Number	Shows the sequential number of the LSA.
Checksum	Shows the checksum of the LSAs.
Length	Shows the length (in bytes) of the LSA.
Network Mask	Shows the network mask of the route corresponding to the LSA.
Metric Type	Shows the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Shows 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 is 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	Shows the router ID.
Type-7 AS External Link States	Shows the type 7 autonomous external LSA information.
LS age	Shows the keepalive period of the LSA.
Options	Option
LS Type	Shows the type of the LSA.
Link State ID	Shows the link ID of the LSA.
Advertising Router	Shows the device advertising the LSA.
LS Seq Number	Shows the sequence number of the LSA.
Checksum	Shows the checksum of the LSAs.
Length	Shows the length (in bytes) of the LSA.
Network Mask	Shows the network mask of the route corresponding to the LSA.
Metric Type	Shows the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Shows 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 is the output of theshow 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

show ip ospf interface

Use this command to show the OSPF-associated interface information in privileged user mode.

show ip ospf interface [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type	(Optional) type of the specified interface
interface-number	(Optional) number of the specified interface

Defaults N/A

Command Mode Privileged user mode

Usage Guide This command shows the OSPF information on the interface.

Configuration Examples

The following is 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 IDof 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

Command	Description

Commands	N/A	N/A

Platform Description N/A

show ip ospf neighbor

Use this command to show the OSPF neighbor list in privileged user mode.

show ip ospf [*process-id***] neighbor [[detail] | [[***interface-type***

interface-number] [neighbor-id]]]

Parameter Description

Parameter	Description
detail	(Optional) Shows the neighbor details.
interface-type *interface-number*	(Optional) Shows the neighbor information of the specified interface
neighbor-id	(Optional) Shows the information of the specified neighbor

Defaults N/A

Command Mode Privileged user mode

Usage Guide This command shows neighbor information usually used to check whether the OSPF is running normally.

Configuration Examples

The following is the output of the **show ip ospf neighbor** command:

```
Ruijie# show ip ospf neighbor
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
LinkState Request List 0
LinkState Retransmission List 0
Crypt Sequence Number is 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
ThreadLinkState Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timeron
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	Shows the area that learns the neighbor.
via interface	Shows 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 bythe neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected bythe 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 isable to function as the GR Helper of a specified neighbor

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip ospf route

Use this command to show the OSPF routes.

show ip ospf [*process-id***] route [count]**

Parameter Description

Parameter	Description
process-id	OSPF process ID. All OSPF routes will be shown without an ID specified.
count	Statistics of various OSPF routes

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command shows the OSPF routing information. The count option shows the OSPF routing statistics.

Configuration Examples

Ruijie# show ip ospf route

```
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 fileds 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

show ip ospf spf

Command

Use this command to show the routing count in the OSPF area.

show ip ospf [*process-id***] spf**

Parameter Description

Parameter	Description
process-id	OSPF process ID

Command Mode Privileged user mode

Usage Guide This command shows the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.

Configuration Examples

The following is 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	Shows the OSPF summary.

Platform Description N/A

show ip ospf summary-address

Use this command to show the converged route of all redistributed routes in privileged user mode.

show ip ospf [*process-id*] **summary-address**

Parameter Description

Parameter	Description
process-id	ID of the OSPF process. All OSPF routing processes will be shown if this parameter is not configured.

Defaults

Command Mode

Privileged user mode

Usage Guide

This command is valid only on the NSSA ABR, and shows only the routes with local aggregation operations.

Configuration Examples

The following is 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 Description

N/A

show ip ospf virtual-link

Use this command to show the OSPF virtual link information in privileged user mode.

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 shown if this parameter is not configured.
ip-address	Associated ID of a virtual link neighbor

Defaults N/A

Command Mode Privileged user mode

Usage Guide If no virtual link is configured, the command shows the neighbor status and other related information. The show ip ospf neighbor command does not show 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	Shows the virtual link neighbors and their status.
Virtual Link State	Shows the virtual link state.
Transit area	Shows the transit area of the virtual link.
via interface	Shows the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Shows 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

OSPFv3 Commands

area authentication

Use this command to enable OSPFv3 area authentication in routing process configuration mode. Use the **no** form of this command to disable OSPFv3 area authentication.

area *area-id* **authentication ipsec spi** *spi* [**md5 | sha1**] [**0 | 7**] *key*

no area *area-id* **authentication**

Parameter Description

Parameter	Description
area-id	Stub area id which can be specified as an interger or an IPv4 prefix.
spi	Security parameter index within the range from 256 to 4294967295.
md5	Adopts Message Digest 5 (MD5) authentication mode.
sha1	Adopts Secure Hash Algorithm 1 (SHA1) authentication mode.
0	Specifies the key to be displayed as plain text.
7	Specifies the key to be displayed as cipher text.
key	Authentication key.

Defaults Authentication is disabled.

Command mode Routing process configuration mode

Usage Guide

The RGOS software supports three authentication modes:

- No authentication is required when this command is not configured;
- MD5 authentication mode;
- SHA1 authentication mode.

OSPFv3 area authentication is effective for all interfaces except the virtual link in this area but interface configuration authentication has a higher priority.

Configuration Examples The following example sets area 1 to adopt MD5 authentication in OSPFv3 routing process configuration mode with key aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-router)# area 1 authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf authentication	Defines interface authentication.
area virtual-link authentication	Defines virtual link authentication.

Platform Description N/A

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 it to the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

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 of 1 to 16777214.

Default configuration

By default, the **default-cost** is 1.

Command mode

Routing process configuration mode.

Usage guidelines

This command can only work in the ABR connected to the stub area.

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	Set a stub area.

Platform Description

None

Command History

Version	Description
-	-

area encryption

Use this command to enable OSPFv3 area encryption and authentication in routing process configuration mode. Use the **no** form of this command to disable OSPFv3 area encryption and authentication.

area *area-id* **encryption ipsec spi** *spi* **esp null** [**md5** | **sha1**] [**0** | **7**] *key*

no area *area-id* **encryption**

Parameter Description

Parameter	Description
area-id	Stub area id which can be specified as an interger or an IPv4 prefix.
spi	Security parameter index within the range from 256 to 4294967295.
null	Adopt null encryption mode.
md5	Adopts Message Digest 5 (MD5) authentication mode.
sha1	Adopts Secure Hash Algorithm 1 (SHA1) authentication mode.
0	Specifies the key to be displayed as plain text.
7	Specifies the key to be displayed as cipher text.
key	Authentication key.

Defaults Encryption and authentication are disabled.

Command mode Routing process configuration mode

Usage Guide The RGOS software supports one encryption mode and two authentication modes:

One encryption mode:

- MULL encryption.

Two authentication modes:

- MD5 authentication mode;
- SHA1 authentication mode.

OSPFv3 area encryption and authentication is effective for all interfaces except the virtual link in this area but interface configuration authentication has a higher priority.

Configuration Examples The following example sets area 1 to adopt null encryption and MD5 authentication in OSPFv3 routing process configuration mode with key aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

```
Ruijie(config-router)# area 1 encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf encryption	Defines interface encryption and authentication.
area virtual-link encryption	Defines virtual link encryption and authentication.

Platform Description N/A

area-range

Use this command to set the range of the converged inter-area addresses. Use the **no** form of this command to remove the setting or restore it to 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	Advertise the range of converged addresses.
not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.

Default configuration

No converged inter-area address range is defined.

Command mode

Routing process configuration mode

Usage guidelines

This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. The routing information combination only takes place on the area border. The specific routing information is seen on the intra-area routers, but only one converged route can be seen on the devices in other areas. By configuring the two options of advertise and not-advertise, you can decide whether to advertise the convergence range to enable blocking and filtering. By default, the range is advertised to the outside. The option cost can be used to set the metric value of convergence routing.

A number of route convergence commands can be defined. In this way, the number of the routes in the OSPF AS is reduced. Particularly for a large network, the forwarding performance will be improved.

When a number of routes are converged, and the containment relationship exists between items, the area range converged is determined by the longest match principle.

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	Set the range of the external routes to be converged.

Platform Description

None

Command History

Version	Description
-	-

area stub

Use this command to create a stub area or set its attributes. Use the **no** form of this command to restore the stub area to an ordinary area or delete its configuration.

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.

Default configuration

No stub area is defined

Command mode

Routing process configuration mode

Usage guidelines

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.

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	Set the cost of the default route in the stub area.

Platform Description

None

Command History	Version	Description
	-	-

area virtual-link

Use this command to create a virtual link or set its parameters. Use the **no** form of this command to delete the virtual link or restore it to the default setting.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*] [**authentication ipsec spi** *spi* [**md5 | sha1**] [**0 | 7**] *key*] [**encryption ipsec spi** *spi* **esp null** [**md5 | sha1**] [**0 | 7**] *key*]

no area *area-id* **virtual-link** *router-id* [**hello-interval**] [**dead-interval**] [**retransmit-interval**] [**transmit-delay**] [**instance**] [**authentication**] [**encryption**]

Parameter description

Parameter	Description
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*	Set the interval to send the hello message on the local virtual link interface in the range from 1 to 65535s.
dead-interval *seconds*	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. Its range is 1 to 65535s.
retransmit-interval *seconds*	Interval for retransmitting LSA on the local interface of the virtual link . The range is from 1 to 65535s.
transmit-delay *seconds*	Delay on the local interface of the virtual link in sending LSA. The range is from 1 to 65535s.
instnace *instance-id*	Specify 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*	Defines OSPFv3 authentication. Note: Authentication between neighbors must be the same. Use the service password-encryption command to display the key as cipher text. *spi*: security parameter index within the ragne from 256 to 4294967295. **md5**: specifies md5 authentication mode. **sha1**: specifies sha1 authentication mode. **0**: specifies the key to be displayed as plain text. **7**: specifies the key to bedisplayed as cipher text. *key*: authentication key.
encryption ipsec spi *spi*	Defines OSPFv3 authentication.

esp null [**md5** | **sha1**] [**0** | **7**] *key*	 Note Authentication between neighbors must be the same. Use the service password-encryption command to display the key as cipher text. *spi*: security parameter index within the ragne from 256 to 4294967295. **null**: specifies null encryption mode.. **md5**: specifies md5 authentication mode. **sha1**: specifies sha1 authentication mode. **0**: specifies the key to be displayed as plain text. **7**: specifies the key to bedisplayed as cipher text. *key*: authentication key.

Default configuration

No virtual link is defined. hello-interval: 10 seconds; dead-interval: four times of the hello-interval; retransmit-interval: 5 seconds; transmit-interval: 1 second. Encryption and authentication are disabled.

Command mode

Routing process configuration mode

Usage guidelines

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.


Caution

- 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.

Examples

The following example configures a virtual link.

```
ipv6 router ospf 1
area 1 virtual-link 192.1.1.1
```

Related commands

Command	Description
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.
show ipv6 ospf virtual-links	Show the OSPFv3 virtual link information.

Platform Description

None

Command History

Version	Description
-	-

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 disable the bandwidth-based interface metric calculation or restore it to the default reference bandwidth.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter description

Parameter	Description
reference-bandwidth *ref-bw*	Reference bandwidth in the range of 1 to 4294967 Mbps.

Default configuration

The interface metric is calculated based on the reference bandwidth, which is 100Mbps.

Command mode

Routing process configuration mode

Usage guidelines

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.

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	Set the cost of an interface.
show ipv6 ospf	Show the OSPFv3 routing process information.

Platform Description

None

Command History

Version	Description
-	-

bdf all-interfaces(OSPFv3)

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. The no form of this command restores it to the default setting.

bdf all-interfaces

no bdf all-interfaces

Parameter description

Parameter	Description
-	-

Default configuration

Disabled.

Command mode

Routing process configuration mode.

Usage guidelines

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.

Examples

N/A

Related commands

Command	Description
ipv6 router ospf *process-id*	Enable the OSPFv3 routing process and enter into the routing process configuration mode.
ipv6 ospf bfd [disable]	Enable or disable the BFD on the specified OSPFv3 interfaces.

Platform Description

None

Command History

Version	Description
-	-

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 ranging from 1 to 65535

Defaults

None

Command Mode

Privileged mode

Usage guidelines

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.

Examples

The example below restarts the OSPF process.

```
enble
clear ipv6 ospf process
```

Related Commands

Command	Description
-	-

Platform Description

None

Command History

Version	Description
-	-

default-information originate

Use this command to generate a default route to the OSPFv3 routing domain in the routing process mode. The **no** form of this command disables the default route.

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 settings

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, with the valid range of 0 to 16777214, 1 by default
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. The external route of type 1 is more trustworthy than that of type 2.

route-map *map-name*	Associated route-map name, no associated route-map by default

Default

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 guideline

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 show 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 shows only the type 1 route.

The routers in the stub area cannot generate external default routes.

Examples

The configuration example below generates a default route.

```
default-information originate always
```

Related commands

Command	Description
redistribute	Redistribute routes.
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf database	Show the OSPFv3 link state database information.

Platform Description

None

Command History

Version	Description
-	-

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 it to 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 1 to 16777214.

Default configuration

20.

Command mode

The default route type is type 2.

Usage guidelines

This command can be used together with **redistribute** to set the default metric for the routes to be redistributed. But this command does not appliy 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.

Examples

The following example sets the default metric for the routes to be redistributed to 10.

```
default-metric 10
```

Related commands

Command	Description
redistribute	Redistribute the routes.
show ipv6 ospf	Show the OSPFv3 routing process information.

Platform Description

None

Command History

Version	Description
-	-

distance

Use this command to set the management distance corresponding to different types of OSPFv3 routes. The **no** form of this command restores it to the defualt setting.

distance {*distance* **| ospf { intra-area** *distance* **| inter-area** *distance* **| external** *distance* **}}**

no distance [ospf]

Parameter description

Parameter	Description
distance	Set the management distance of the route, in the range of 1 to 255.
intra-area *distance*	Set the management distance of the intra-area route, in the range of 1 to 255.
inter-area *distance*	Set the management distance of the inter-area route, in the range of 1 to 255.
external *distance*	Set the management distance of the external route, in the range of 1 to 255.

Default

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 guidelines

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.

Examples

In the configuration below, the OSPFv3 external route management distance is set to 160.

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# distance ospf external 160
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process .

Platform Description

None

Command History

Version	Description

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 disable this function.

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*	Configure the specific OSPFv3 instance on the interface.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

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.

Examples

The following example starts the OSPFv3 process on int fastethernet 0/0 for the specified area of the specified instance.

```
int fastethernet 0/0
ipv6 ospf 1 area 2 instance 2
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
passive-interface	Set the a passive interface.
show ipv6 ospf interface	Show the OSPFv3 interface information.

Platform Description

None

Command

Version	Description

History	-	-

ipv6 ospf authentication

Use this command to enable OSPFv3 interface authentication in interface configuration mode. Use the **no** form of this command to disable OSPFv3 interface authentication.

ipv6 ospf authentication [**null** | **ipsec spi** *spi* [**md5** | **sha1**] [**0** | **7**] *key*] [**instance** *instance-id*]

no ipv6 ospf authentication [**instance** *instance-id*]

Parameter Description

Parameter	Description
null	No authentication.
spi	Security parameter index within the range from 256 to 4294967295.
md5	Adopts Message Digest 5 (MD5) authentication mode.
sha1	Adopts Secure Hash Algorithm 1 (SHA1) authentication mode.
0	Specifies the key to be displayed as plain text.
7	Specifies the key to be displayed as cipher text.
key	Authentication key.
instance *instance-id*	Specifies an OSPFv3 instance on the interface within the range from 0 to 255.

Defaults Authentication is disabled.

Command mode Interface configuration mode

Usage Guide The RGOS software supports three authentication modes:

- No authentication is required when this command is not configured;
- MD5 authentication mode;
- SHA1 authentication mode.

OSPFv3 interface authentication requires configuration of the same authentication parameters on the connected interfaces.

Configuration Examples The following example shows how to adopt MD5 authentication in OSPFv3 interface configuration mode with key aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-if)# ipv6 ospf authentication ipsec spi 300 md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
area authentication	Defines area authentication.
area virtual-link authentication	Defines virtual link authentication.

Platform N/A

Description

ipv6 ospf bdf

Use this command to enable or disable the BFD on the specifed OSPFv3-enabled interface. The **no** form of this command is used to remove the setting on the interface.

ipv6 ospf bfd [**disable**] [**instance** *instance-id*]

no ipv6 ospf bfd [**instance** *instance-id*]

Parameter description

Parameter	Description
disable	Disable the BFD function on the specified OSPF interface.
instance *instance-id*	Configure the specified OSPFv3 instance on the interface, in the range of 0 to 255.

Default configuration No configuration is made by default. The BFD configuration in the OSPFv3 process configuration mode will apply.。

Command mode Interface configuration mode.

Usage guidelines 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.

Examples N/A

Related commands

Command	Description
ipv6 router ospf *process-id*	Start the OSPFv3 routing process and enter into the routing process configuration mode.
bdf all-interfaces	Enable the BFD on all OSPFv3 interfaces.

Platform Description None

Command History

Version	Description
-	-

ipv6 ospf cost

Use this command to set the cost of the interface. Use the **no** form of this command to restore it to 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. Its range is 1 to 65535.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface, which ranges from 0 to 255.

Default configuration

The default interface cost is the reference bandwidth/Bandwidth (100Mbps by default).

Command mode

Interface configuration mode.

Usage guidelines

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.

Examples

The following example sets the cost of the interface to 1:

```
ipv6 ospf cost 1
```

Related commands

Command	Description
show ipv6 ospf interface	Show the OSPFv3 interface information.
ipv6 ospf area	Set the interface to participate in the OSPFv3 routing process.

Platform Description

None

Command

Version	Description

History		

ipv6 ospf dead-interval

Use this command to set the interval for the interface to consider that the neighbor fails. If the interface receives no hello message from the neighbor during the interval, it considers that the neighbor fails. Use the **no** form of this command to restore it to 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 1 to 65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface, which ranges from 0 to 255.

Default configuration

Four times the value of **ipv6 ospf hello-interval.**

Command mode

Interface configuration mode.

Usage guidelines

The dead interval of neighbors shall be the same. Otherwise the normal adjacency will not be established.

By default, the dead interval is four times the hello sending interval. If the hello interval changes, the dead interval changes accordingly.

It's not recommended to modify the parameter directly. If needed, note that:

- The dead interval shall be larger than the interval for senting hello packets by the neighbor.
- The same dead interval shall be set for the neighbors.

Examples

The following example sets the dead interval considered by the local interface to 60s.

```
ipv6 ospf dead-interval 60
```

Related commands

Command	Description
ipv6 ospf hello-interval	Set the interval for sending the Hello message on an interface.
show ipv6 ospf interface	Show the OSPFv3 interface information.
ipv6 ospf area	Set the interface to participate in the OSPFv3 routing process

Platform Description

None

Command History

Version	Description
-	-

ipv6 ospf mtu-ignore

Use this command to ignor the MTU check when an interface receives the database description message. The **no** form of this command is used to restore it to the default.

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter description

Parameter	Description
instance *instance-id*	Configure the specific OSPFv3 instance on the interface, in the range of 0 to 255.

Default The MTU check is enabled by default。

Command mode Interface configuration mode.

Usage guidelines 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.

Examples The configuration example below 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	Start the OSPFv3 routing process.
ipv6 mtu	Set the value of IPv6 MTU of the interface.

Platform Description None

Command History

Version	Description
-	-

ipv6 ospf encryption

Use this command to enable OSPFv3 interface encryption and authentication in interface configuration mode. Use the **no** form of this command to disable OSPFv3 interface encryption and

authentication.

ipv6 ospf authentication [**null** | **ipsec spi** *spi* [**md5** | **sha1**] [**0** | **7**] *key*] [**instance** *instance-id*]

no ipv6 ospf authentication [**instance** *instance-id*]

Parameter Description

Parameter	Description
null	No authentication.
spi	Security parameter index within the range from 256 to 4294967295.
null	Adopts null encryption mode.
md5	Adopts Message Digest 5 (MD5) authentication mode.
sha1	Adopts Secure Hash Algorithm 1 (SHA1) authentication mode.
0	Specifies the key to be displayed as plain text.
7	Specifies the key to be displayed as cipher text.
key	Authentication key.
instance *instance-id*	Specifies an OSPFv3 instance on the interface within the range from 0 to 255.

Defaults Encryption and Authentication are disabled.

Command mode Interface configuration mode

Usage Guide The RGOS software supports one encryption mode and two authentication modes:

One encryption mode:

- MULL encryption.

Two authentication modes:

- MD5 authentication mode;
- SHA1 authentication mode.

OSPFv3 interface authentication requires configuration of the same authentication parameters on the connected interfaces.

Configuration Examples The following example shows how to adopt null encryption and MD5 authentication in OSPFv3 interface configuration mode with key aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
Ruijie(config-if)# ipv6 ospf encryption ipsec spi 300 esp null md5
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
area encryption	Defines area encryption and authentication.
area virtual-link encryption	Defines virtual link encryption and authentication.

Platform Description N/A

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 it to 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 1-65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration 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 guidelines The same hello sending intervals must be set for the neighbors, otherwise the normal adjacency cannot be established.

Examples The following example sets the interval for the interface to send the Hello message to 20s.

```
ipv6 ospf hello-interval 20
```

Related commands

Command	Description
ipv6 ospf dead-interval	Set the interval for the interface to consider that the neighbor fails.
show ipv6 ospf interface	Show the OSPFv3 interface information.
ipv6 ospf area	Set the interface to participate in the OSPFv3 routing process.

Platform Description None

Command History

Version	Description
-	-

ipv6 ospf neighbor

Use this command to configure the OSPFv3 neighbor manually. Use the **no** form of this command to restore it to 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) Configure 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) Configure 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) Configure 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 guidelines

You can set relevant parameters for the neighbors depending on the actual network type.

Configuration Examples

The configuration example below configures 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	Set the priority value of an interface.
Ipv6 ospf network	Set the network type of an interface.

Platform Description

None

Command History

Version	Description
-	-

ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore it to 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	Specify the broadcast network type.
non-broadcast	Specify the non-broadcast network type.
point-to-point	Specify the point-to-point network type.
point-to-multipoint	Specify the point-to-multipoint network type.
point-to-multipoint non-broadcast	Specify the point-to-multipoint non-broadcast network type.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface with the valid id range of 0-255.

Default configuration

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

You can set the network type of the interface according to the actual link type applied and the

guidelines topology.

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	Set the interface priority.
show ipv6 ospf interface	Show the OSPFv3 interface information.
ipv6 ospf area	Set the interface to participate in the OSPFv3 routing process.

Platform Description None

Command History

Version	Description
-	-

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 0 to 255.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface. Its range is 0 to 255.

Default configuration 1.

Command mode Interface configuration mode.

Usage guidelines 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.

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	Set the network type of an interface.
router-id	Set the ID of a router.
show ipv6 ospf interface	Show the OSPFv3 interface information.
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Platform Description

None

Command History

Version	Description
-	-

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 it to 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 1 to 65535(s).
instance *instance-id*	Configure the specific OSPFv3 instance on the interface.

Default configuration

5 seconds.

Command mode

Interface configuration mode.

Usage guidelines

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.

Examples

The following example sets the interval for retransmitting the LSA to 10s.

```
ipv6 ospf retransmit-interval 10
```

Related

Command	Description

commands	**show ipv6 ospf interface**	Show the OSPFv3 interface information.
	ipv6 ospf area	Set the interface to participate in the OSPFv3 routing process.

Platform Description None

Command History	**Version**	**Description**
	-	-

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 it to 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 1 to 65535(s).
	instance *instance-id*	Configure the ID of a specific OSPFv3 instance on the interface, with a range of 0-255.

Default configuration 1 second.

Command mode Interface configuration mode.

Usage guidelines Use this command to set the delay on the interface in transmitting the LSA.

Examples The following example sets the delay on the interface in transmitting the LSA.

```
ipv6 ospf transmit-delay 2
```

Related commands	**Command**	**Description**
	show ipv6 ospf interface	Show the OSPFv3 interface information.

Platform Description None

Command	**Version**	**Description**

History	-	-

ipv6 router ospf

Use this command to start the OSPFv3 routing process. Use the **no** form of this command to disable the OSPFv3 routing process.

ipv6 router ospf *[process-id]*

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.

Default configuration No OSPFv3 routing process is started.

Command mode Global configuration mode.

Usage guidelines After the OSPFv3 process is started, the routing process configuration mode is entered.
At present, our products support up to 32 OSPFv3 processes.

Examples The following example starts the OSPFv3 process.

```
ipv6 router ospf 1
```

Related commands

Command	Description
ipv6 ospf area	Configure an interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Show the OSPFv3 routing process information.

Platform Description None

Command History

Version	Description
-	-

ipv6 router ospf max-concurrent-dd

Use this command to set the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes.

ipv6 router ospf max-concurrent-dd *number*

no ipv6 router ospf max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum concurrent interacting neighbors Range: 1.-65535

Defaults 5, by default

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 example below 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 are allowed on this device.

```
Ruijie#conf terminal
Ruijie(config)#ipv6 router ospf max-concurrent-dd 4
```

Related Commands

Command	Description
max-concurrent-dd	Set the maximum concurrent interacting neighbors in the OSPFv3 processes

Platform Description None

Command History

Version	Description
10.4(3)	Newly added command

log-adj-changes

Use this command to enable the logging of adjacency changes. The **no** and **default** form of the command is used to disable it.

log-adj-changes

no log-adj-changes

Parameter

Parameter	Description

Description		
	detail	Show 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 None

Configuration Examples The configuration example below 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	Show the OSPF global configuration information

Platform Description None

Command History	Version	Description
	-	-

max-concurrent-dd

Use this command to set the maximum number of DD packets that can be processed concurrently in the OSPFv3 routing process.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter description	Parameter	Description
	number	Maximum number of DD packets that can be processed concurrently, with a range of 1-65535.

Default configuration 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.

Examples

The example below 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 are allowed on this device.

```
router ipv6 ospf 1
max-concurrent-dd 4
```

Related Commands

Command	Description
ipv6 router ospf max-concurrent-dd	Set the maximum concurrent interacting neighbors allowed in the OSPFv3 processes.

Platform Description

None

Command History

Version	Description
-	-

passive-interface

Use this command to set the passive interface. Use the **no** form of this command to remove the configuration .

passive-interface {**default** | *interface-type interface-number* }

no passive-interface {**default** | *interface-type interface-number* }

Parameter description

Parameter	Description
default	Set all the interfaces to passive ones.
interface-type interface-number	Set the specified interface to a passive one.

Default configuration

No passive interface is set.

Command mode

Routing process configuration mode

Usage guidelines

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.

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	Configure an interface to participate in the OSPFv3 routing process.
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.

Platform Description

None

Command History

Version	Description
-	-

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 disable this function or modify the redistribution parameters.

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*	Specify 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*	Specify 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*	Specify the tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.

Default configuration

The function is not enabled;
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 guidelines

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.


Caution

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 can not 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

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	Set the default route to be redistributed.
default-metric	Set the default metric for the route to be redistributed.
summary-prefix	Set the converged address range of the external route.
show ipv6 ospf	Show the OSPFv3 routing process information.
show ipv6 ospf database	Show the OSPFv3 link state database information.

Platform Description

None

Command History

Version	Description
-	-

router-id

Use this command to set the router ID (device ID). Use the **no** form of this command to remove the setting or restore it to the default router ID.

router-id *router-id*

no router-id

Parameter description

Parameter	Description
router-id	ID of the device in the IPv4 address format.

Default configuration

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

Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the

guidelines 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

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	Set the interface priority.
show ipv6 ospf	Show the OSPFv3 routing process information.

Platform Description None

Command History

Version	Description
-	-

summary-prefix

Use this command to configure the converged route outside the OSPFv3 routing domain in the routing process configuration mode. The **no** form of this command is used to restore it to the default setting.

summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise | tag** <*0-4294967295*>]

no summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise | tag** <*0-4294967295*>]

Parameter description

Parameter	Description
ipv6-prefix/*prefix-length*	Address range of the converged route
not-advertise	Do not advertise the converged route to neighbors. Absence of this parameter means to advertise.
tag<*0-4294967295*>	Tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.

Default No converged route is configured by default.

Command mode Routing process configuration mode.

Usage guidelines When routes are redistributed by another routing process into the OSPFv3 routing process, every route is advertised to the OSPFv3-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous system border device can advertise only

one converged route, thus reducing the scale of routing table greatly.

It is different from the **area range** command. The area range involves the convergence of routes between OSPFv3 areas, while the **summary-prefix** involves the convergence of external routes of the OSPFv3 routing domain.

The **summary-prefix** command is valid only on the ASBR now, and causes the convergence for only redistributed routes.

Examples

The example below configures the external route within the 2001:DB8::/64 to the converged route 2001:DB8::/64 to advertise it.

```
summary-prefix 2001 :DB8 : : /64
```

Related commands

Command	Description
area-range	Configure route convergence between the OSPFv3 areas.
redistribute	Redistribute the routes in other routing process.

Platform Description

None

Command History

Version	Description
-	-

Timers spf

Use this command to set the delay and interval for the OSPFv3 to calculate SPF after receiving the topology change. The **no** format of this command is used to restore it to the default.

timers spf *delay holdtime*

no timers spf

Parameter description

Parameter	Description
spf-delay	Define 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	Define 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.

Default configuration

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 guidelines

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.

Examples

The configuration example below 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	Restart part of the function of the OSPFv3.
show ipv6 ospf	Show the OSPFv3 routing process information.
timers throttle spf	Configure the exponential backoff delay of the SPF calculation

Platform Description None

Command History

Version	Description
-	-

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 the topology change information for OSPFv3 in the routing process configuration mode. The **no** form of this command restores it to default.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter description

Parameter	Description
spf-delay	Define the SPF calculation waiting period, in milli-seconds, with the valid range from 1 to 600000. After receiving the topology change information, the OSPFv3 routing process must wait for the specified period of *spf-delay* before starting the SPF calculation.
spf-holdtime	Define the minimum interval between two SPF calculations, in

	milli-seconds, with the valid range from 1 to 600000.
spf-max-waittime	Define the maximum interval between two SPF calculations, in milli-seconds, with the valid range from 1 to 600000.

Default spf-delay: 1000ms; spf-holdtime: 5000ms; spf-max-waittime: 10000ms.

Command mode Routing process configuration mode.

Usage guidelines

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.

Note

- 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

Examples

The configuration example below 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: 5ms，1s，3s，7s，15s，31s，63s，89s，179s，179+90 ……

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# timers throttle spf 5 1000 90000
```

Related commands

Command	Description
clear ipv6 ospf	Restarts part of the OSPFv3 function.
show ipv6 ospf	Show the routing process information of the OSFPv3
timers spf	Configure the SPF calculation delay .

Platform Description	None

Command History	**Version**	**Description**

show ipv6 ospf

Use this command to show the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter description	**Parameter**	**Description**
	process- id	OSPF process ID number.

Defaults	None
Command mode	Privileged EXEC mode.
Usage Guide	None

Examples

The following example shows 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
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 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 device 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
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 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 device 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	Start the OSPFv3 routing process.
default-information originate	Set the default route to be redistributed.
default-metric	Set the default metric for the route to be redistributed.
router-id	Set the OSPFv3 routing process ID
timers spf	Set the delay and the minimum and maximum intervals for the OSPFv3 to perform SPF calculation after receiving the topology change information.

Platform Description

None

Command History

Version	Description
-	-

show ipv6 ospf database

Use this command to show 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 shown.
adv-router *router-id*	Show the LSA information generated by the specified router.

Defaults None

Command mode Privileged EXEC mode.

Usage Guide None

Examples

The following example shows 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	Start the OSPFv3 routing process.

Platform Description None

Command History	Version	Description
	-	-

show ipv6 ospf interface

Use this command to show the OSPFv3 interface information.

show ipv6 ospf interface [*interface-type interface-number*]

Parameter description	Parameter	Description
	interface-type interface-number	Specify the interface type and interface number.

Defaults None

Command mode Privileged EXEC mode.

Usage Guide None

Examples

The following commands show 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 shown. 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	Start the OSPFv3 routing process.
ipv6 ospf area	Enable the interface to participate in the OSPFv3 process.

Platform Description None

Command History

Version	Description

show ipv6 ospf neighbor

Use this command to show the neighbor information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **neighbor** [**interface-type** *interface-number* [**detail**]| *neighbor-id* |**detail**]

Parameter description

Parameter	Description
process- id	OSPFv3 process ID number
detail	Show details about the neighbor.
interface-type interface-number	Interface type and interface number
neighbor-id	Neighbor's router ID

Defaults None

Command mode Privileged EXEC mode.

Usage Guide None

Examples

The following command shows 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 shows 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	Start the OSPFv3 routing process.
ipv6 ospf area	Enable the interface to participate in the OSPFv3 process.
area virtual-link	Configure the OSPFv3 virtual link.
show ipv6 ospf interface	Show the OSPFv3 interface information.

Platform Description None

Command History	Version	Description
	-	-

show ipv6 ospf route

Use this command to show 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 None

Command mode Privileged EXEC mode.

Usage Guide None

Examples The following example shows 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	Start the OSPFv3 routing process.

Platform Description None

Command History	Version	Description

show ipv6 ospf summary-prefix

Use this command to show 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 None

Command mode Privileged EXEC mode.

Usage Guide None

Examples The following command shows 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	Start the OSPFv3 routing process.
	summary-prefix	Configure the converge route outside the OSPFv3 routing domain.

Platform Description None

Command History	Version	Description
	-	-

show ipv6 ospf topology

Use this command to show 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 None

Command mode Privileged EXEC mode.

Usage Guide None

Examples

The following command shows 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   --
```

Related commands

Command	Description
ipv6 router ospf	Start the OSPFv3 routing process.
area range	Configure the address range of the OSPF area.

Platform Description None

Command History

Version	Description
-	-

show ipv6 ospf virtual-links

Use this command to show 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 None

Command mode Privileged EXEC mode.

Usage Guide None

Examples The following command shows 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	Start the OSPFv3 routing process.
area virtual-link	Configure the OSPFv3 virtual link.
show ipv6 ospf neighbor	Show the OSPFv3 neighbor information.

Platform Description None

Command History

Version	Description
-	-

ospfv3 help

Use this command to show the typical configuration of OSPFv3 modules.

ospfv3 help

Parameter description

Parameter	Description
-	-

Default configuration N/A

Command mode Privileged EXEC mode.

Usage guidelines

This command is used to show the typical configuration of OSPFv3 modules.

The information shown of the command is as follows:

```
Ruijie#ospfv3 help

-------------------------------- Example Menu --------------------------------
1.Basic OSPFv3 configuration example
2.Static route redistribution configuration example
3.OSPFv3 Stub area configuration example

------------------------------------------------------------------------------
Please select the number you want to view (Press the ESC to exit):
```

Examples

```
Ruijie#ospfv3 help

-------------------------------- Example Menu --------------------------------
1.Basic OSPFv3 configuration example
2.Static route redistribution configuration example
3.OSPFv3 Stub area configuration example

------------------------------------------------------------------------------
Please select the number you want to view (Press the ESC to exit): 1

-------------------------- Configuration Requirements --------------------------
Enable the OSPFv3 protocol on the routing device A and B. Configure the IP
address range and area associated with this routing process and establish
the OSPFv3 neighbors.

------------------------------ Configuration Steps ------------------------------
Device A Configuration:
Ruijie(config)#ipv6 router ospf  1
//Create the OSPFv3 process 1 and enter the OSPFv3 routing configuration mode.
Ruijie(config-router)#router-id 1.1.1.1
//Set the router-id of the OSPFv3 process 1 as 1.1.1.1

Ruijie(config)#interface gigabitEthernet 0/1
//Enter the interface configuration mode.
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 enable
//Enable the IPv6 on the interface.
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 address 3001::1/64
//Configure the IPv6 address of the interface.
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0
//Enable the OSPFv3 on the interface, add the interface to the OSPFv3 process 1
in the area 0.

Device B Configuration:
Ruijie(config)#ipv6 router ospf  1
//Create the OSPFv3 process 1 and enter the OSPFv3 routing configuration mode.
Ruijie(config-router)#router-id 2.2.2.2
//Set the router-id of the OSPFv3 process 1 as 2.2.2.2

Ruijie(config)#interface gigabitEthernet 0/1
//Enter the interface configuration mode.
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 enable
//Enable the IPv6 on the interface.
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 address 3001::2/64
//Configure the IPv6 address of the interface.
Ruijie(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0
//Enable the OSPFv3 on the interface, add the interface to the OSPFv3 process 1
in the area 0.

------------------------------------------------------------------------------


Ruijie#
```

```
Ruijie#ospfv3 help

--------------------------------- Example Menu ---------------------------------
1.Basic OSPFv3 configuration example
2.Static route redistribution configuration example
3.OSPFv3 Stub area configuration example

--------------------------------------------------------------------------------
Please select the number you want to view (Press the ESC to exit): 2

-------------------------- Configuration Requirements --------------------------
Configure a static route and redistribute it to the OSPFv3 process.

------------------------------ Configuration Steps -----------------------------
Ruijie(config)#ipv6 route 2001:db8:77::/48 2001:db9::1
//Configure the static route.

Ruijie(config)#ipv6 router ospf 1
//Create the OSPFv3 process 1 and enter the OSPFv3 routing configuration mode.
Ruijie(config-router)#redistribute static
//Redistribute the static route.

--------------------------------------------------------------------------------


Ruijie#

Ruijie#ospfv3 help

--------------------------------- Example Menu ---------------------------------
1.Basic OSPFv3 configuration example
2.Static route redistribution configuration example
3.OSPFv3 Stub area configuration example

--------------------------------------------------------------------------------
Please select the number you want to view (Press the ESC to exit): 3

-------------------------- Configuration Requirements --------------------------
Configure the OSPFv3 protocol according to the following topology, where in the
A/B/C are routing devices, and A is the ABR. Set the area1 as the (Totally)
Stub area.
        .....C.............A.............B.....
                Area 1            Area 0


------------------------------ Configuration Steps -----------------------------
Device A Configuration:
Ruijie(config)#ipv6 router ospf 1
//Create the OSPFv3 process 1 and enter the OSPFv3 routing configuration mode.
Ruijie(config-router)#area 1 stub no-summary
//Set the area 1 as the (Totally) Stub area.

Device C Configuration:
Ruijie(config)#ipv6 router ospf 1
//Create the OSPFv3 process 1 and enter the OSPFv3 routing configuration mode.
Ruijie(config-router)#area 1 stub
//Set the area 1 as the (Totally) Stub area.

--------------------------------------------------------------------------------


Ruijie#
```

Note:Use the *language chinese/english* command in privileged EXEC mode to switch between the Chinese and the English interfaces.

Related commands

Command	Description
view ospfv3	Show the main status and configuration information of OSPFv3 modules.

Platform None

Description

Command History	Version	Description
	10.4(3)	Newly added command

view ospfv3

Use this command to show the main status and configuration information of OSPFv3 modules.

view ospfv3

Parameter description	Parameter	Description
	-	-

Default configuration

N/A

Command mode

Any mode.

Usage guidelines

This command is used to show the main status and configuration information of OSPFv3 modules.

Examples

The information shown of the command is as follows:

```
Ruijie#view ospfv3

OSPFv3 Processes:4
Process ID Router ID       ABR ASBR Areas LSAs   Routes Nbrs(All/Full) IFs
---------- --------------- --- ---- ----- ------ ------ -------------- ----
1          192.168.1.1     Y   Y    10    10000  10000  100/80         100
2          192.168.2.1     Y   N    10    10000  10000  100/80         100
65534      192.168.3.1     Y   N    10    10000  10000  100/80         100
......
---------- --------------- --- ---- ----- ------ ------ -------------- ----
Total                      4   2    40    40000  40000  400/320        400
More information, refer to: show ipv6 ospf

OSPFv3 Max Concurrent DD: 20
OSPFv3 down due to insufficient memory and will be restarting in 60s.

Ruijie#
```

Related commands	Command	Description
	ospfv3 help	Show the typical configuration information of OSPFv3 modules.

Platform Description

None

Command	Version	Description

History		
	10.4(3)	Newly added command

area help

Use this command to show the example information of the commands beginning with the keyword **area**.

area help

Parameter description	Parameter	Description
	-	-

Default configuration

N/A

Command mode

Routing process configuration mode.

Usage guidelines

This command is used to show the example information of the commands beginning with the keyword area.

Examples

The information shown of the command is as follows:

```
Ruijie(config-router)#area help

Examples:
--------------------------------------------------------------------------------
>area 1 default-cost 5

Set the metric of the default route in the Stub area 1 as 5.
1: area ID;                          5: default routing metric;
--------------------------------------------------------------------------------
>area 1 range fec0::/48

Set the range of the aggregation addresses in the area 1 as fec0::/48.
1: area ID;
fec0::/48: range of the aggregation addresses
--------------------------------------------------------------------------------
>area 1 stub

Configure the area 1 as the stub area.
--------------------------------------------------------------------------------
>area 1 virtual-link 192.168.2.1

Configure the virtual link on the neighbor routing device 192.168.2.1 in area 1.
1: area ID;
192.168.2.1: identifier of the neighbor routing device;
--------------------------------------------------------------------------------

Ruijie(config-router)#
```

Note:Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
area default-cost	Configure the metric of the default route.
area range	Configure the area range.
area stub	Configure the stub area.

area virtual-link	Configure the virtual link.

Platform Description None

Command History

Version	Description
10.4(3)	Newly added command

default-information help

Use this command to show the example information of the commands beginning with the keyword **default-information**.

default-information help

Parameter description

Parameter	Description
-	-

Default configuration N/A

Command mode Routing process configuration mode.

Usage guidelines This command is used to show the example information of the commands beginning with the keyword default-information.

Examples

The information shown of the command is as follows

```
Ruijie(config-router)#default-information help

Examples:
------------------------------------------------------------------------------
>default-information originate always metric 5

Always generate an external default route, with metric 5.
always: Generate a default route, no matter whether the default local route
exists or not.
5: metric of the generated default route (default: 1);
------------------------------------------------------------------------------
>default-information originate metric-type 1 route-map myrmap

If the default local route exists and its attributes meet the route map mymap,
 a default route with metric type 1 will be introduced.
1: metric type(default: 2);             myrmap: route map name;
------------------------------------------------------------------------------

Ruijie(config-router)#
```

Note:Use the language chinese/english command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
default-information	Introduce the external default route.

Platform Description None

Command History

Version	Description
10.4(3)	Newly added command

ipv6 ospf help

Use this command to show the example information of the commands beginning with the keyword **ipv6 ospf**.

ipv6 ospf help

Parameter description

Parameter	Description
-	-

Default configuration N/A

Command mode Interface configuration mode.

Usage guidelines This command is used to show the example information of the commands beginning with the keyword ipv6 ospf.

Examples

The information shown of the command is as follows

```
Ruijie(config-if)#ipv6 ospf help

Examples:
--------------------------------------------------------------------------------
>ipv6 ospf 1 area 10 instance 3

Add the interface to the OSPFv3 process 1 in the area 10, and the instance 3.
1: OSPFv3 process ID;                    10: OSPFv3 area ID;
3: instance ID;
--------------------------------------------------------------------------------
>ipv6 ospf network point-to-point

Set the OSPFv3 nework type as point-to-point.
--------------------------------------------------------------------------------
>ipv6 ospf priority 10

Set the OSPFv3 priority as 10 (default: 1)
--------------------------------------------------------------------------------

Ruijie(config-if)#
```

Note:Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
ipv6 ospf area	Enable the OSPFv3 on an interface.
ipv6 ospf network	Configure the network type for the interface.

ipv6 ospf priority	Configure the interface priority.

Platform Description None

Command History

Version	Description
10.4(3)	Newly added command

ipv6 ospf network help

Use this command to show the example information of the commands beginning with the keyword **ipv6 ospf network**.

ipv6 ospf network help

Parameter description

Parameter	Description
-	-

Default configuration N/A

Command mode Interface configuration mode.

Usage guidelines This command is used to show the example information of the commands beginning with the keyword ipv6 ospf network.

The information shown of the command is as follows:

Examples

```
Ruijie(config-if)#ipv6 ospf network help

Example:
------------------------------------------------------------------------------
>ipv6 ospf network point-to-point

Set the OSPFv3 network type as point-to-point.
------------------------------------------------------------------------------

Ruijie(config-if)#
```

Note: Use the *language chinese/english* command in privileged EXEC mode to switchover the Chinese/English interface

Related commands

Command	Description
ipv6 ospf network	Configure the network type for the interface.

Platform Description None

Command History

Version	Description
10.4(3)	Newly added command

ipv6 ospf priority help

Use this command to show the example information of the commands beginning with the keyword **ipv6 ospf priority**.

ipv6 ospf priority help

Parameter description

Parameter	Description
-	-

Default configuration

N/A

Command mode

Interface configuration mode.

Usage guidelines

This command is used to show the example information of the commands beginning with the keyword ipv6 ospf priority.

Examples

The information shown of the command is as follows

```
Ruijie(config-if)#ipv6 ospf priority help

Example:
--------------------------------------------------------------------------------
>ipv6 ospf priority 10

Set the OSPFv3 priority as 10 (default: 1)
--------------------------------------------------------------------------------

Ruijie(config-if)#
```

Note: Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
ipv6 ospf priority	Configure the interface priority.

Platform Description

None

Command History

Version	Description
10.4(3)	Newly added command

ipv6 router ospf help

Use this command to show the example information of the commands beginning with the keyword **ipv6 router ospf**.

ipv6 router ospf help

Parameter description

Parameter	Description
-	-

Default configuration

N/A

Command mode

Global configuration mode.

Usage guidelines

This command is used to show the example information of the commands beginning with the keyword ipv6 router ospf.

Examples

The information shown of the command is as follows

```
Ruijie(config)#ipv6 router ospf help

Example:
------------------------------------------------------------------------------
>ipv6 router ospf 1

Create the OSPFv3 routing process1 and enter the OSPFv3 routing configuration
mode.
------------------------------------------------------------------------------

Ruijie(config)#
```

Note: Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
ipv6 router ospf	Configure the OSPFv3 routing process.

Platform Description

None

Command History

Version	Description
10.4(3)	Newly added command

ipv6 ospf process-id area help

Use this command to show the example information of the commands beginning with the keyword **ipv6 ospf process-id area**.

ipv6 ospf *process-id* **area help**

Parameter description	Parameter	Description
	process-id	Ospf process id, within the range of 1 to 65535.

Default configuration

N/A

Command mode

Interface configuration mode.

Usage guidelines

This command is used to show the example information of the commands beginning with the keyword ipv6 ospf process-id area.

Examples

The information shown of the command is as follows:

```
Ruijie(config-if)#ipv6 ospf 1 area help

Example:
--------------------------------------------------------------------------------
>ipv6 ospf 1 area 10 instance 3

Add the interface to the OSPFv3 process1 in the area 10, and the instance 3.
1: OSPFv3 process ID              10: OSPFv3 area ID
3: instance ID
--------------------------------------------------------------------------------

Ruijie(config-if)#
```

Note: Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
ipv6 ospf area	Enable the OSPFv3 on the interface.

Platform Description

None

Command History

Version	Description
10.4(3)	Newly added command

redistribute help

Use this command to show the example information of the commands beginning with the keyword **redistribute**.

redistribute help

Parameter description	Parameter	Description
	-	-

Default configuration	N/A
Command mode	Routing process configuration mode.
Usage guidelines	This command is used to show the example information of the commands beginning with the keyword redistribute.

Examples	The information shown of the command is as follows
	`Ruijie(config-router)#redistribute help`
	
	`Examples:`
	`--------------------------------------------------------------------------------`
	`>redistribute static metric 30`
	
	`Redistribute the static routes and set the metric as 30.`
	`static: redistribute the static routes;`
	`30: metric of the redistributed route;`
	`--------------------------------------------------------------------------------`
	`>redistribute rip metric-type 1`
	
	`Redistribute the RIP routes and set the metric type as 1`
	`rip: redistribute the RIP route;`
	`1: metric type of the redistributed route (default: 2);`
	`--------------------------------------------------------------------------------`
	`>redistribute bgp route-map myrmap tag 24`
	
	`Redistribute the BGP routes that meet the route map "myrmap" and set the tag as 24.`
	`bgp: redistribute the BGP route; myrmap: route map name;`
	`24: tag value of the redistributed route;`
	`--------------------------------------------------------------------------------`
	
	`Ruijie(config-router)#`
	Note: Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands	**Command**	**Description**
	redistribute	Configure the redistribution.

Platform Description	None

Command History	**Version**	**Description**
	10.4(3)	Newly added command

route-id help

	Use this command to show the example information of the commands beginning with the keyword **route-id**. **route-id help**

Parameter	**Parameter**	**Description**

description	-	-

Default configuration N/A

Command mode Routing process configuration mode.

Usage guidelines This command is used to show the example information of the commands beginning with the keyword route-id.

Examples The information shown of the command is as follows:

```
Ruijie(config-router)#

Ruijie(config-router)#router-id help

Example:
--------------------------------------------------------------------------------
>router-id 192.168.1.1

Set the router ID as 192.168.1.1
--------------------------------------------------------------------------------
```

Note: Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
route-id	Configure the router ID.

Platform Description None

Command History

Version	Description
10.4(3)	Newly added command

summary-prefix help

Use this command to show the example information of the commands beginning with the keyword **summary-prefix**.

summary-prefix help

Parameter description

Parameter	Description
-	-

Default configuration N/A

Command Routing process configuration mode.

mode

Usage guidelines

This command is used to show the example information of the commands beginning with the keyword summary-prefix.

Examples

The information shown of the command is as follows:

```
Ruijie(config-router)#summary-prefix help

Example:
--------------------------------------------------------------------------------
>summary-prefix 2001:db8:77::/48 tag 32

Configure the aggregation range of external route as 2001:db8:77::/48 and set
the aggregated route tag as 32.
2001:db8:77::/48: aggregation range of the external route
32: tag value of the aggregated route
--------------------------------------------------------------------------------

Ruijie(config-router)#
```

Note: Use the *language chinese/english* command in the privileged EXEC mode to switch between the Chinese and English interfaces.

Related commands

Command	Description
summary-prefix	Configure the external route summary.

Platform Description

None

Command History

Version	Description
10.4(3)	Newly added command

BGP4 Commands

address-family ipv4

Use this command to enter "address-family IPv4" to configure BGP configuration mode. Use the **exit-address-family** 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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv4
```

Related Commands

Command	Description
exit-address-family	Exits the mode.

Platform Description

N/A

address-family ipv4 vrf

Use this command to enter the address-family IPv4 VRF configuration mode to configure BGP and enable the exchange of route information of a VRF. Use the **no** form of this command to disable the exchange function or the **exit-address-family** command to exit BGP address configuration mode.

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

```
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 This command is supported on RSR20, RSR30, RSR50, and RSR50E series routers.

address-family ipv6

Use this command to enter "address-family IPv6" of BGP configuration mode and enable the exchange of IPv6 route information. The **no** form of this command disables this function. Use the exit-address-family command to exit BGP address-family configuration mode.

address-family ipv6 [**unicast** | **multicast**]

no address-family ipv6 [**unicast** | **multicast**]

Parameter Description

Parameter	Description
unicast	Optional, enters IPv6 unicast address-family configuration mode.
multicast	Optional, enters IPv6 multicast 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.
You can enter the multicast mode to configure the BGP of the multicast topology, which is used for RPF detection of the IPv6 multicast routing protocol.
The **exit-address-family** command is used to return to BGP configuration mode.

Configuration Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family ipv6
```

Related Commands

Command	Description
exit-address-family	Exits the mode.

Platform Description N/A

address-family vpnv4

Use this command to enter address-family VPN configuration mode and enable the exchange of VPN route information between PE peers. Use the **exit-address-family** command to exit BGP address configuration mode.

address-family vpnv4 [**unicast**]

no address-family vpnv4 [**unicast**]

Parameter Description

Parameter	Description
unicast	Optional, detailed IPv4 unicast address prefix

Defaults No VPN address family is defined by default.

Command Mode BGP configuration mode

Usage Guide
Execute this command to enter address-family VPN configuration mode and enable the exchange of VPN route information between PE peers.
To return to BGP configuration mode, run the command exit-address-family

Configuration Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# address-family vpnv4
```

Related Commands

Command	Description
exit-address-family	Exits the mode.

Platform Description This command is supported only on appliances that support the MPLS function.

aggregate-address (IPv4)

Use this command to set the aggregate IPv4 route. The **no** form of the command is used to disable this function.

aggregate-address *ip-address mask* [**as-set**] [**summary-only**]

no aggregate-address *ip-address mask* [**as-set**] [**summary-only**]

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.

Defaults The address aggregation is not configured by default.

Command Mode BGP configuration mode, address-family IPv4 configuration mode, or address-family IPv4 VRF 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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# aggregate-address 10.0.0.0
255.0.0.0 as-set
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

Platform Description N/A

aggregate-address (IPv6)

Use this command to set the aggregate IPv6 route. The **no** form of the command is used to disable this function.

aggregate-address *ipv6-network / length* [**as-set**] [**summary-only**]

no aggregate-address *ipv6-network / length* [**as-set**] [**summary-only**]

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.

Defaults The address aggregation is not configured by default.

Command Mode BGP IPv6 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

```
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 N/A

bgp always-compare-med

Use this command to compare Multi Exit Discriminator (MED) all the time. Use the **no** form of the command to disable this function.

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

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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp always-compare-med
```

Related Commands

Command	Description
show ip bgp	Shows 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

N/A

bgp asnotation dot

Use this command to modify the showing 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). You can use the **no** form of the command to disable this function.

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

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 shows 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 shown. 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 show the 4-byte AS notation, both modes can be used when entering the configuration commands. But the representation and showing 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

```
Ruijie(config)# router bgp 1.0
Ruijie(config-router)# bgp asnotation dot
```

Related Commands

Command	Description
show ip bgp summary	Shows the related information of BGP neighbor.

Platform Description N/A

bgp bestpath as-path ignore

Use this command to disregard the length of the AS path. Use the **no** form of the command to disable this function.

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

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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath as-path ignore
```

Related Commands

Command	Description
show ip bgp	Shows the BGP route entry.

Platform Description	N/A

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. The **no** form of the command is used to disable this function.

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

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

```
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	N/A

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 the command to disable this function.

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

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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath compare-confed-aspath
```

Related Commands

Command	Description
show ip bgp	Shows the BGP route entry.
bgp router-id	Sets the BGP Device ID.

Platform Description

N/A

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 the command to disable this function.

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

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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath compare-routerid
```

Related Commands

Command	Description
show ip bgp	Shows the BGP route entry.
bgp router-id	Sets the BGP Device ID.

Platform Description N/A

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 the command to disable this function.

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

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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath med confed
```

Related Commands

Command	Description
show ip bgp	Shows 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 N/A

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 the command to disable this function.

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

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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# bgp bestpath medmissing-as-worst
```

Related Commands

Command	Description
show ip bgp	Shows the BGP route entry.
bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
bgp bestpath med confed	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform Description N/A

bgp client-to-client reflection

Use this command to enable the route reflection function between clients on the device. The **no** form of the 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

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

```
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 N/A

bgp cluster-id

Use this command to configure the cluster ID of the route reflector. Use the **no** form of the 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

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

```
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 N/A

bgp confederation identifier

Use this command to configure the AS confederation identifier. Use the **no** form of the 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 1 to 4294967295, which is represented as 1 to 65535.65535 in dot mode.

Defaults There is no confederation identifier by default

Command Mode BGP configuration mode

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

```
Ruijie(config-router)# bgp confederation identifier 65000
```

Related Commands

Command	Description
bgp confederation peers	Adds member AS of the AS confederation.

Platform Description

N/A

bgp confederation peers

Use this command to configure member ASs of the AS confederation. The **no** form of the command deletes the configured member AS.

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 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.


Note

This command can configure up to 15 members of a confederation at one time. For more members, enter them for several times.

Configuration Examples

```
Ruijie(config-router)# bgp confederation peers 65000 65100
```

Related Commands

Command	Description
bgp confederation identifier	Configures the confederation identifier.

Platform Description

N/A

bgp dampening

Use this command to enable the routing attenuation and set the attenuation parameters in the address-family or routing configuration mode. The no form of this command is used to remove the setting.

bgp dampening [*half-life* [*reusing suppressing duration*] | **route-map** *name*]

no bgp dampening [*half-life* [*reusing suppressing duration*] | **route-map** [*name*]]

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, or BGP L2VPN VPLS/VPWS 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

```
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	Shows the suppressed route information.

Platform Description

N/A

bgp default ipv4-unicast

Use this command to set the IPv4 unicast address as the default address family. The **no** form of the command removes the configuration.

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 by default.

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

```
Ruijie(config-router)# default ipv4-unicast
```

Related Commands

Command	Description
address-family ipv4	Enters the IPv4 address mode.

Platform Description	N/A

bgp default local-preference

Use this command to set the default local-preference attribute value. Use the **no** form of the command to restore the defaults.

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 is100 by default.
Command Mode	BGP 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	`Ruijie(config-router)# bgp default local-preference 200`

Related Commands

Command	Description
show ip bgp	Shows 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	N/A

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 the command to disable this function.

bgp default route-targe filter

no bgp default route-targe filter

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Mode BGP configuration mode or VPNv4 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

```
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 This command is supported only on appliances that support the BGP MPLS/VPN function.

bgp deterministic-med

This command sets 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. The **no** form of the command turns off it.

bgp deterministic med

no bgp deterministic med

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The function is disabled by default.

Command Mode BGP configuration mode

Usage Guide They will be compared with each other according to the sequence the paths are received when the optimal path is selected by default. Execute the following operations in the BGP configuration mode to compare paths of peers from the same AS firstly:

Configuration Examples

```
Ruijie(config-router)# bgp deterministic med
```

Related Commands

Command	Description
show ip bgp	Shows 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 N/A

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. The **no** form of the command disables the 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

```
Ruijie(config-router)# bgp enforce-first-as
```

Related Commands

Command	Description
show ip bgp	Shows the BGP route entry.

Platform Description	N/A

bgp fast-external-fallover

When the network interface used in establishing the connection of the directly-connected EBGP peer fails, this command is used to establish the BGP session connection quickly. Use the **no** form of the 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	`Ruijie(config-router)# bgp faster-external-fallover`

Related Commands	**Command**	**Description**
	router bgp	Enables the BGP protocol.

Platform Description	N/A

bgp graceful-restart

Use this command to enable the graceful restart function of the global BGP. The **no** form of the command is used to disable this function.

bgp graceful-restart

no bgp graceful-restart

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

Defaults	The default BGP cannot enable the graceful restart function and cannot help neighbors to perform

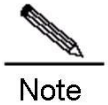
graceful restart.

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. Currently, for the Ruijie devices, only the S8600 and S9600 products support the continuous forwarding of the IPv4 unicast address-family and the IPv6 unicast address-family, While other BGP devices with the GR function enabled could only help the BGP restart device performing the graceful-restart.

Configuration Examples

```
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

bgp graceful-restart restart-time

Use this command to configure the restart time of the BGP graceful-restart. The **no** form of the command restores the default value.

bgp graceful-restart restart-time *restart-time*

no bgp graceful-restart restart-time

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 seconds.

Parameter Description

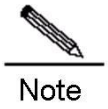
Defaults The restart time is 120 seconds by default.

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.


Note

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

```
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

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. The **no** form of the command restores the stalepath-time to the default value.

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 seconds

Defaults The time is 360 seconds by default.

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

```
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

bgp log-neighbor-changes

Use this command to log the BGP status changes without turning on debug. Use the **no** form of the 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

```
Ruijie(config-router)# bgp log-neighbor-changes
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

Platform Description N/A

bgp maxas-limit

Use this command to set maximum AS amount in the route AS-PATH attributes when BGP receives a route from its neighbor. Use the **no** form of the command to restore the default setting.

bgp maxas-limit *number*

no bgp maxas-limit

Parameter Description

Parameter	Description
number	Maximum AS amount in AS-PATH attributes within the ranges from 1 to 512.

Defaults The AS amount is not restricted in the route AS-PATH attributes

Command mode BGP configuration mode or BGP Scope Global configuration mode

Usage Guide This command is used to set maximum AS amount in the route AS-PATH attributes when BGP receives a route from its neighbor. A route with an AS amount exceeding the configured limit will be discarded directly.

After the configuration is changed, the user needs to reconfigure BGP neighbors with the **clear** command manually to enable this command.

Configuration Examples

```
Ruijie(config-router)# bgp maxas-limit 100
```

Related Commands	Command	Description
	clear bgp all	Reconfigures all BGP neighbors,

Platform Description N/A

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 the 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 seconds

Defaults The delay time is 5 seconds by default.

Command Mode BGP configuration mode, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF 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

```
Ruijie(config-router)# bgp nexthop trigger delay 30
```

Related Commands	Command	Description
	bgp nexthop trigger enable	Enables the nexthop trigger.

Platform Description N/A

bgp nexthop trigger enable

Use this command to enable the nexthop trigger update function. Use the **no** form of the 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, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF configuration mode

Usage Guide This command is used to enable the nexthop trigger update function.

Configuration Examples

```
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 N/A

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.

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, address-family IPv4/IPv6 configuration mode, address-family IPv4 VRF configuration mode

Usage Guide This command is used to control whether IBGP routes are allowed to be redistributed to the IGP protocol.

Configuration Examples

```
Ruijie(config-router)# bgp redistribute-internal
```

Related Commands

Command	Description
redistribute	Redistributes routes learned from other protocols.

Platform Description	N/A

bgp router-id

Use this command to configure the ID-IP address of the device. The **no** form of the command restores the default IP address.

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

```
Ruijie(config-router)# bgp router-id 10.0.0.1
```

Related Commands

Command	Description
show ip bgp dampening dampened-paths	Shows the suppressed routing information.
bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform Description	N/A

bgp scan-rib disable

Use this command to configure the timely scan for the BGP protocol to update the routing table. The **no** form of this command cancels the timely scan.

bgp scan-rib disable

no bgp scan-rib disable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode BGP configuration mode, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config-router)# bgp scan-rib disable
```

Related Commands	Command	Description
	bgp scan-time	Configures the interval for the BGP timely scan.

Platform Description N/A

bgp scan-time

Use this command to configure the interval for the BGP timely scan.

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 seconds

Defaults The scan time is 60 seconds by default.

Command Mode BGP configuration mode, address-family IPv4/IPv6/VPNv4 configuration mode, address-family IPv4 VRF 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

```
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	N/A

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 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 seconds.

Defaults The delay time is 120 seconds by default.

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 The following example sets the update-delay time to 200 seconds.

Examples

```
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 N/A

clear bgp all

Use this command to reset all BGP address-families. The content to be reset depends on the parameters behind.

clear bgp all [*as number*]

clear bgp all peer-group *peer-group-name* [[**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 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.
peer-group	Resets the specified peer group.
peer-group-name	Name of the peer group
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 N/A

clear bgp ipv4 mdt

Use this command to reset the IPv4 mdt address-family of BGP.

This command has the similar function with the **clear bgp ipv4 unicast** command except for the operation address family.

Parameter Description	Parameter	Description
	Refer to the **clear bgp ipv4 unicast** command.	Refers to the **clear bgp ipv4 unicast** command.

Defaults Refer to the **clear bgp ipv4 unicast** command.

Command Mode Privileged EXEC mode

Usage Guide Refer to the **clear bgp ipv4 unicast** command.

Configuration Examples N/A

Related Commands	Command	Description
	clear bgp ipv4 unicast	Resets the IPv4 unicast address-family.

Platform Description N/A

clear bgp ipv4 unicast

Use this command to reset the IPv4 address-family of BGP. This command has the same function and parameter with the **clear ip bgp** command.

Parameter Description	Parameter	Description
	Refer to the **clear ip bgp** command.	Refers to the **clear ip bgp** command.

Defaults Refer to the **clear ip bgp** command.

Command Mode	Privileged EXEC mode
Usage Guide	Refer to the **clear ip bgp** command.
Configuration Examples	N/A

Related Commands

Command	Description
clear ip bgp	Resets the IPv4 unicast address-family.

Platform Description	N/A

clear bgp ipv4 unicast dampening

Use this command to clear the dampening information and release suppressed routes.

clear bgp ipv4 unicast dampening [*address* [*mask*]]

Parameter Description

Parameter	Description
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

```
Ruijie# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related Commands

Command	Description
show ip bgp dampening dampened-paths	Shows the suppressed routing information.
bgp dampening	Enables the route dampening and sets the dampening parameters.

Platform Description N/A

clear bgp ipv4 unicast external

Use this command to reset all EBGP connections.

clear bgp ipv4 unicast external [[**soft**] [**in** | **out**]]

Parameter Description

Parameter	Description
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

```
Ruijie# clear bgp ipv4 unicast external in
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.

show ip bgp neighbors	Shows the neighbor information.

Platform Description N/A

clear bgp ipv4 unicast flap-statistics

Use this command to clear the route oscillation statistics.

clear bgp ipv4 unicast flap-statistics [*address*[*mask*]]

Parameter Description

Parameter	Description
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

```
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	Shows the BGP route entry.

Platform Description N/A

clear bgp ipv4 unicast peer-group

Use this command to reset the session with all members in the peer group.

clear bgp ipv4 unicast peer-group *peer-group-name* [[**soft**] [**in** | **out**]]

Parameter Description

Parameter	Description
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

```
Ruijie# clear bgp ipv4 unicast peer-group my-group in
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Shows the BGP route entry.

Platform Description N/A

clear bgp ipv6 unicast

Use this command to reset the BGP IPv6 unicast address-family.

This command is similar to the **clear bgp ipv4 unicast** command except that it is executed in a different address-family.

Parameter Description

Parameter	Description
Please refer to the **clear bgp ipv4 unicast** command.	Please refer to the **clear bgp ipv4 unicast** command.

Defaults Please refer to the **clear bgp ipv4 unicast** command.

Command Mode Privileged EXEC mode

Usage Guide Please refer to the **clear bgp ipv4 unicast** command.

Configuration Examples	N/A

Related Commands	**Command**	**Description**
	clear bgp ipv4 unicast	Reset the IPv4 unicast address-family.

Platform Description	N/A

clear bgp vpnv4 unicast

Use this command to reset the BGP VPNV4 unicast address-family.

This command is similar to the **clear bgp ipv4 unicast** except that it is executed in a different address-family.

Parameter Description	**Parameter**	**Description**
	Please refer to the **clear bgp ipv4 unicast** command.	Please refer to the **clear bgp ipv4 unicast** command.

Defaults	Please refer to the **clear bgp ipv4 unicast** command.
Command Mode	Privileged EXEC mode
Usage Guide	Please refer to the **clear bgp ipv4 unicast** command.
Configuration Examples	N/A

Related Commands	**Command**	**Description**
	clear bgp ipv4 unicast	Resets the IPv4 unicast address-family.

Platform Description	N/A

clear ip bgp

Use this command to reset the BGP session.

clear ip bgp {* | *as number* } [[**soft**] [**in** | **out**]]

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

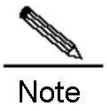
Usage Guide

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.


Note

All connected BGP routers must support the route refresh function to execute this command. This product supports the route refresh function.

Configuration Examples

```
Ruijie# clear bgp ipv4 unicast *
```

Related Commands

Command	Description
neighbor soft-reconfiguration inbound	(Optional) Restarts the BGP session and reserves the unchanged route information sent by the BGP peer (group).
show ip bgp	Shows the BGP route entry.

Platform Description	N/A

clear ip bgp dampening

Use this command to clear the dampening information and release suppressed routes.

clear ip bgp dampening [*address mask*]

Parameter Description

Parameter	Description
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 BGP route dampening.

Configuration Examples

```
Ruijie# clear ip bgp dampening 192.168.0.0 255.255.0.0
```

Related Commands

Command	Description
show ip bgp dampening dampened-paths	Shows the suppressed routing information.
bgp dampening	Enables the route dampening function and sets dampening parameters.

Platform Description	N/A

clear ip bgp external

Use this command to reset all EBGP connections.

clear ip bgp external [[**soft**] [**in** | **out**]]

Parameter Description

Parameter	Description
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

```
Ruijie# clear ip bgp external in
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp neighbors	Shows the neighbor information.

Platform Description N/A

clear ip bgp flap-statistics

Use this command to clear the routes vibration statistics of the IPv4 unicast address family.

clear ip bgp flap-statistics [*address*[*mask*]]

Parameter Description

Parameter	Description
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

```
Ruijie# clear ip bgp flap-statistics
```

Related Commands	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
	show ip bgp	Shows the BGP route entry.

Platform Description N/A

clear ip bgp peer-group

Use this command to reset the session with all members in the peer group.

clear ip bgp peer-group *peer-group-name* [[**soft**] [**in** | **out**]]

Parameter Description	Parameter	Description
	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

```
Ruijie# clear ip bgp peer-group my-group in
```

Related Commands	Command	Description
	clear ip bgp	Resets the BGP session.
	show ip bgp	Shows the BGP route entry.

Platform Description N/A

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

```
Ruijie# clear ip bgp table-map
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Shows the BGP route entry.

Platform Description N/A

clear ip bgp vrf

Use this command to reset sessions of all the members in VRF.

clear ip bgp vrf *vrf-name* [* *address* }[**soft** [**in** | **out**]]

Parameter Description

Parameter	Description
vrf-name	VRF name
*	Resets all the current BGP sessions.
address	Resets the BGP session with the specified peer.
in	Without parameter **soft**, resets the direct session with the specific peer.
out	Without parameter **soft**, resets the direct session with the BGP speaker.
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 BGP sessions of all the members in VRF.

Configuration Examples

```
Ruijie# clear ip bgp vrf my-vrf in
```

Related Commands

Command	Description
clear ip bgp	Resets the BGP session.
show ip bgp	Shows the BGP route entry.

Platform Description This command is supported on RSR20, RSR30, RSR50, and RSR50E series routers.

default-information originate

Use this command to enable BGP to distribute the default route. The **no** form of this command is used to disable the distribution of the default route.

default-information originate

[no] default-information originate

Parameter Description

Parameter	Description
N/A	N/A

Defaults The redistributed default route is not distributed externally.

Command Mode BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, BGP IPv4 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

```
Ruijie(config-router)# default-information originate
```

Related Commands

Command	Description
network	Configures routes to be advertised.
redistribute	Redistributes routes of other protocol.

Platform Description N/A

default-metric

Use this command to set the metric for route redistribution. The **no** form of this command is used to remove the configuration and restore the default value.

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.


Note

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

```
Ruijie(config-router)# default-metric 45
```

Related Commands

Command	Description
redistribute	Redistributes routes of other protocol.

Platform Description N/A

distance bgp

Use this command to set different management distances for different types of BGP routes. The no command is used 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. Range: 1 to 255

Defaults

The parameter defaults are as follows:
external-distance - 20
internal-distance - 200
local-distance - 200

Command Mode

BGP 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

```
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	Shows the BGP route entry.

Platform Description

N/A

exit-address-family

Use this command to exit BGP address-family configuration mode.

exit-address-family

Parameter Description

Parameter	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

```
Ruijie(config-router-af)#exit-address-family
```

Related Commands

Command	Description
address-family ipv4	Enters address-family ipv4 configuration mode.

Platform Description N/A

ip as-path access-list

Use this command to specify the regular expression based AS path filtering rule. The **no** command is used to delete the rule.

ip as-path access-list *path-list-num* {**permit** | **deny**} *regular-expression*

no ip as-path access-list *path-list-num*

Parameter Description

Parameter	Description
path-list-num	Name of the AS path control list based on the regular expression in the range from 1 to 500
permit	Permits access.
deny	Denies access.
regular-expression	Regular expression Range: 1 to 255 characters.

Defaults N/A

Command Mode	Global configuration mode
Usage Guide	For the regular expression, see Configuring IP Unicast Route.
Configuration Examples	`Ruijie(config)# ip as-path access-list 105 deny ^123$`

Related Commands

Command	Description
neighbor filter-list	Applies the AS-path access control list on the specified peer.
neighbor distribute-list	Applies the distribution list on the specified peer.

Platform Description	None

Command History

Version	Description
N/A	N/A

maximum-paths ebgp

Use this command to configure the number of cost-equal paths for the EBGP multipathing load balancing function. The **no** form of the command is used to disable the EBGP multipathing load balancing function.

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 ECMP is not supported by default.
Command Mode	BGP configuration mode, BGP IPv4 address-family configuration mode, and BGP IPv6 address-family 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	`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

maximum-paths ibgp

Use this command to configure the number of cost-equal paths for the IBGP multipathing load balancing function. The **no** form of the command is used 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 IBGP ECMP is not supported by default.

Command Mode BGP configuration mode, BGP IPv4 address-family configuration mode, and 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

```
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 Description N/A

maximum-prefix

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 value.

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, 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 VPNv4 configuration mode, or 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 show 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.


Note

When the address family is overflow as the number of prefixes reaches the maximum number, you can adjust maximum-prefix.


Caution

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

The following example sets the maximum number of prefixes in the BGP routing database in the ipv4

Examples 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 < *addressfamily*|**all**> *****	Resets the BGP address-family.
show bgp < *addressfamily* **| all** > **summary**	Shows the summary of BGP address-family.

Platform Description N/A

neighbor activate

Use this command to activate the neighbor or peer group in the current address mode. Use the **no** form of the command to restore the default setting.

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 It is enabled by default in address-family IPv4 configuration mode

Command Mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 configuration mode

Usage Guide The function is enabled by default for IPv4 address families. You need to set this command in other address-family configuration modes for exchanging routes.

Configuration Examples

```
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

neighbor advertisement-interval

Use this command to set the time interval to send the BGP route update message. Use the **no** form of the 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

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

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router)# neighbor 10.0.0.1 advertisement-interval 10
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description

N/A

neighbor allowas-in

Use this command to allow the PE to receive messages with the same AS number as itself. The **no** form restores the default value.

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, address-family IPv4 configuration mode, or address-family IPv4 VRF 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

```
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 N/A

neighbor as-override

Use this command to allow the PE to override the AS number of a site. The **no** form restores the default value.

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 address-family IPv4 VRF 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

```
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 N/A

neighbor default-originate

Use this command to allow the BGP speaker to advertise the default route to the peer (group). The **no** form of the command removes the configuration.

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

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

```
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 N/A

neighbor description

Use this command to set a descriptive sentence for the specified peer (group). The **no** form of the command removes the 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

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

```
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 N/A

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. The **no** form of the command removes the configured ACL.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and address-family VPNv4 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

```
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 N/A

neighbor ebgp-multihop

Use this command to allow establishing BGP connection between EBGP peers that are not directly connected. The **no** form of the command removes the 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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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

```
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

N/A

neighbor filter-list

Use this command to enable route filtering when sending/receiving routing information to/from BGP peers. The **no** form of the command cancels the filtering.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, and 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

```
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 N/A

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. The no form of this command deletes the local AS.

neighbor {*peer-address* | *peer-group-name*} **local-as** *as-number* [**no-prepend** [**replace-as** [**dual-as**]]]

no neighbor {*peer-address* | *peer-group-name*} **local-as**

Parameter Description

Parameter	Description
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 1 to 4294967295, represented as 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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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 andcorresponding 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

```
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

neighbor maximum-prefix

Use this command to limit the number of prefixes received from the specified BGP peer. The no form of the command removes the configured limitation.

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	Do 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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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	`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	N/A

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 the command to remove the configuration.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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	`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 N/A

neighbor next-hop-unchanged

Use this command to maintain the next-hop when sending routes to the peer(group). Use the **no** form of the command to remove the configuration.

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	Maintain 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, address-family IPv4 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

```
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

N/A

neighbor password

When the BGP connection with the BGP peer is established, use this command to enable TCP MD5 authentication and set the password. The **no** form of the command disables MD5 authentication.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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

```
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 N/A

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 delete the specified BGP peer from the peer group.

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

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, advertisemet-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.

Note Do not place neighbors of different address families in the same peer group, or place IBGP and EBGP neighbors in the same peer group.

Configuration Examples

```
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	Shows the information of the BGP peer.

Platform Description N/A

neighbor peer-group (creating)

Use this command to create a BGP peer group. The **no** form of the command deletes the specified peer group and all its members.

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

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

```
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	Shows the information of the BGP peer.

Platform Description N/A

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. The **no** form of the command removes the prefix-list configured.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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

```
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

N/A

neighbor remote-as

Use this command to configure the BGP peer (group). The **no** form of the command deletes the configured peer (group).

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 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.

Defaults No BGP peer is configured.

Command Mode BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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

```
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 N/A

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 the command to remove the configuration.

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 BGP configuration mode, address-family IPv4 configuration mode, address-family IPv6 configuration

Mode mode, or address-family IPv4 VRF 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
```
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 N/A

neighbor route-map

Use this command to enable route match for the received/sent routes. Use the **no** form of the 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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode and address-family IPv4 VPNv4 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
```
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	Shows the BGP route entry.

Platform Description N/A

neighbor route-reflector-client

Use this command to configure the local device as the route reflector and specifies its client. The **no** form of the command removes the client configured.

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 Mode BGP configuration 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

```
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 N/A

neighbor send-community

Use this command to transmit community attributes to the specified BGP neighbor. Use the **no** form of the command to disable this function.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF configuration mode, or address-family IPv4 VPNv4 configuration mode

Usage Guide This command transmits the community to the neighbor or neighbor group.

Configuration Examples

```
Ruijie(config-router)# neighbor 10.1.1.1 send-community both
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.
ip community-list	Creates the community list.

Platform Description N/A

neighbor send-label

Use this command to specify to carry the MPLS label of the route when sending the route to a neighbor. Use the **no** form of the command to disable this function.

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, address-family IPv4 configuration mode and address-family VPNv4 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

```
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 This command is supported only on appliances that support the MPLS function.

neighbor shutdown

Use this command to disconnect the BGP connection established with the specified BGP peer. The **no** form of the command reconnects the BGP peer (group).

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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

```
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	Shows the BGP connection status.

Platform Description

N/A

neighbor soft-reconfiguration inbound

Use this command to store the routing information sent from the BGP peer. Use the **no** form of the command to remove the 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

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

```
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	Shows the information of the BGP peer.
clear ip bgp	Resets the BGP peer session.

Platform Description N/A

neighbor soo

Use this command to set the SOO value of the neighbor. Use the **no** form of the command to remove the configuration.

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 Address-family IPv4 VRF configuration mode

Usage Guide In CE dual-home mode, execute this command to prevent routes sent by CE to PEs from being sent back to CE.

Configuration Examples

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router)# address-family ipv4 vrf vpn1
```

```
Ruijie(config-router)# neighbor 10.0.0.1 soo 100:100
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
timers bgp	Configures the keepalive and holdtime values globally.

Platform Description

N/A

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 the 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

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

```
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

N/A

neighbor unsuppress-map

Use this command to selectively advertise routing information suppressed by aggregate-address command. Use the **no** form of the 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

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

```
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	N/A

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. The **no** form of the command automatically matches the optimal local interface.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, address-family IPv4 VRF 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

```
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	N/A

neighbor version

Use this command to show the number of the BGP protocol version used by the specific BGP neighbor. The **no** form of the command uses the default version number.

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

Usage Guide When the command is used, BGP will lose the version negotiation function.

Configuration Examples

```
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 N/A

neighbor weight

Use this command to set the weight for the specific neighbor. The **no** form of the command removes the 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

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

```
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

N/A

network(BGP)

Use this command to configure the network information to be advertised by the local BGP speaker. The **no** form of the command deletes the configured network information.

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.

Command Mode

BGP 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

```
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	N/A

network synchronization

Use this command to advertise the network information after the local BGP speaker is synchronized with the local device. The **no** form of the command directly advertises 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
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

```
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	N/A

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
no	Disallows BGP to enter the OVERFLOW state when the memory is insufficient.

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

Example 1: When the memory is insufficient, BGP does not enter the OVERFLOW configuration status.

```
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**	Shows the summary of the BGP address family.

Platform Description

N/A

redistribute

Use this to redistribute routes between the other routing protocol and the BGP. The **no** form of the command disables the function.

redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

no redistribute *protocol-type* [**route-map** *map-tag*] [**metric**]

Parameter Description

Parameter	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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, or address-family IPv4 VRF 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

```
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	Shows the protocol configuration.

Platform Description N/A

redistribute ospf

Use this command to redistribute routes between OSPF and BGP. The **no** form of the command disables the function.

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, address-family IPv4 configuration mode, address-family IPv6 configuration mode, or address-family IPv4 VRF 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.


Note

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.


Caution

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

```
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	Shows the protocol configuration.

Platform Description N/A

redistribute isis

Use this command to redistribute routes between ISIS and BGP. The **no** form of the command disables the function and parameter configuration.

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, address-family IPv4 configuration mode, or address-family IPv6 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.


Note

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.


Caution

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

```
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	Shows the protocol configuration.

Platform Description

N/A

router bgp

Use this command to enable the BGP protocol, configure the local autonomous system number and enter BGP protocol configuration mode. The **no** form of the command disables the BGP protocol.

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 1 to 4294967295, represented as 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

```
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

N/A

synchronization

Use this command to enable the synchronization mechanism of BGP and IGP routing information. The **no** form of the command disables the synchronization mechanism of the BGP and IGP routing information.

synchronization

no synchronization

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

BGP 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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# synchronization
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.

Platform Description	N/A

table-map

Use this command to control the route information distributed to the kernel table.

table-map *route-map-name*

no table-map

Parameter Description

Parameter	Description
route-map-name	Name of the route-map

Defaults N/A

Command Mode BGP configuration mode, address-family IPv4 configuration mode, or address-family IPv4 VRF 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

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# table-map bgp_tm
```

Related Commands

Command	Description
route-map	Configures the route-map

Platform Description	N/A

timers bgp

Use this command to adjust the BGP network timer. The **no** form of the command restores 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

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

```
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

N/A

show bgp all

Use this command to show all the address-families information of BGP route. The use of this command is consistent with other BGP's show commands.

Show 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**}]

Show the route dampening parameter.

show bgp all dampening parameters

Show the related information of the neighbors.

show bgp all neighbors.

show bgp all summary

Show 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 Examples None

Related Commands	Command	Description
	show bgp ipv4 unicast	Shows the IPv4 unicast route information of BGP

Platform Description N/A

show bgp ipv4 mdt

Use this command to show the ipv4 mdt routing or neighbor information of all vrfs or rds.

show bgp ipv4 mdt all [*network* | **neighbor** [*address*] | **summary**]

show bgp ipv4 mdt rd *rd_value* [*network*]

Parameter Description	Parameter	Description
	network	Specifies network address.
	neighbor	Shows the neighbor information of the route.
	address	Shows the specific neighbor information.
	summary	Shows the main information of the route.
	rd_value	RD value, such as 100:1 or 202.118.239.165:1

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to show all ipv4 mdt routing information of all vrf or rd.

Configuration Examples

```
Ruijie# show bgp ipv4 mdt 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 ipv4 mdt all summary
BGP router identifier 192.168.183.1, local AS number 23
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

show bgp ipv4 unicast

Use this command to show the IPv4 unicast route information of BGP.

show bgp ipv4 unicast [*network* [*network-mask*]]

show bgp ipv4 unicast community *community-number* [**exact-match**]

show bgp ipv4 unicast community-list *community-name* [**exact-match**]

show bgp ipv4 unicast dampening dampened-paths

show bgp ipv4 unicast dampening flap-statistics

show bgp ipv4 unicast filter-list *path-list-number*

show bgp ipv4 unicast inconsistent-as

show bgp ipv4 unicast prefix-list *ip-prefix-list-name*

show bgp ipv4 unicast quote-regexp *regexp*

show bgp ipv4 unicast regexp *regexp*

show bgp ipv4 unicast route-map *map-tag*

show bgp ipv4 unicast neighbors *neighbor-address* [**received-routes** | **routes** | **advertised-routes**]

show bgp ipv4 unicast cidr-only

show bgp ipv4 unicast labels

Parameter Description

Parameter	Description
network	Shows the specific routing information in the routing table
network-mask	Shows the routing information included in the specified network.
community *community-number*	Shows 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*	Shows the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matching the community value or community-list.
dampening dampened-paths	Shows the restrained routing information.
dampening flap-statistics	Shows the routing dampening statistics.
filter-list *path-list-number*	Shows the routing information matching the filter-list.
inconsistent-as	Shows the routing information of the inconsistent source AS.
prefix-list *ip-prefix-list-name*	Shows the routing information matching the specified prefix-list.
quote-regexp *regexp*	Shows the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp *regexp*	Shows the BGP routing information with the AS path attribute matching the specified regexp.
route-map *map-tag*	Shows the routing information matching the specified route-map filtering condition.
neighbors *neighbor-address* **received-routes**	Shows all routing information received from the specified peer (including the accepted and refused route).
neighbors *neighbor-address* **routes**	Shows all the routing information received from the peer and accepted.
neighbors *neighbor-address* **advertised-routes**	Shows all the routing information sent to the specified peer.
cidr-only	Shows the routing information without the category.
labels	Shows 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 show the matching route information.

Configuration Examples

```
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	Shows the IPv4 unicast route information of BGP.

Platform Description N/A

show bgp ipv4 unicast dampening parameters

Use this command to show the IPv4 unicast route dampening parameters configured for the BGP.

show bgp ipv4 unicast dampening parameters

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to show the IPv4 unicast route dampening parameters configured for BGP.

Configuration Examples

```
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 N/A

show bgp ipv4 unicast neighbors

Use this command to show the related information of BGP IPv4 unicast neighbor.

show bgp ipv4 unicast neighbors *neighbor-address*

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 information of the connection with BGP IPv4 unicast neighbor.

Configuration Examples

```
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 N/A

show bgp ipv4 unicast paths

Use this command to show the path information of the IPv4 unicast in the route database.

show bgp ipv4 unicast 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

```
Ruijie# show bgp ipv4 unicast paths
Address  Refcnt Path
[0x1d7806a0:0] (67)
[0x1d7389a0:13] (20) 10
```

Related Commands	N/A
Platform Description	N/A

show bgp ipv4 unicast summary

Use this command to show the related information of BGP IPv4 unicast.

show bgp ipv4 unicast summary

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

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to show the related information of BGP IPv4 unicast.

Configuration Examples

```
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	N/A

show bgp ipv6 unicast

Use this command to show the IPv6 unicast routing information of BGP.

show bgp ipv6 unicast [*IPv6-Prefix*]

show bgp ipv6 unicast community *community-number* [**exact-match**]

show bgp ipv6 unicast community-list *community-name* [**exact-match**]

show bgp ipv6 unicast dampening dampened-paths

show bgp ipv6 unicast dampening flap-statistics

show bgp ipv6 unicast filter-list *path-list-number*

show bgp ipv6 unicast inconsistent-as

show bgp ipv6 unicast prefix-list *ipv6-prefix-list-name*

show bgp ipv6 unicast quote-regexp *regexp*

show bgp ipv6 unicast regexp *regexp*

show bgp ipv6 unicast route-map *map-tag*

show bgp ipv6 unicast neighbors *neighbor-address*

[**received-routes** | **routes** | **advertised-routes**]

Parameter Description

Parameter	Description
IPv6-prefix	Shows 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*	Shows 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*	Shows the BGP routing information matching the specified community-list.
exact-match	Routing information exactly matches the community value or community-list.
dampening dampened-paths	Shows the restrained routing information.
dampening flap-statistics	Shows the routing dampening statistics.
filter-list *path-list-number*	Shows the routing information matching the filter-list.
inconsistent-as	Shows the routing information of the inconsistent source AS.
prefix-list *ipv6-prefix-list-name*	Shows the routing information matching the specified prefix-list.
quote-regexp *regexp*	Shows the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
regexp *regexp*	Shows the BGP routing information with the AS path attribute matching the specified regexp.
route-map *map-tag*	Shows the routing information matching the specified route-map filtering condition.
neighbors *neighbor-address* **received-routes**	Shows all routing information received from the specified peer (including accepted and refused routes).
neighbors *neighbor-address*	Shows all the routing information received from the peer and

routes	accepted.
neighbors *neighbor-address* **advertised-routes**	Shows 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 show 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	Shows the IPv4 unicast route information of BGP.

Platform Description N/A

show bgp ipv6 unicast dampening parameters

Use this command to show the IPv6 unicast route dampening parameters configured for BGP.

show bgp ipv6 unicast dampening parameters

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to show 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

Field	Description
N/A	N/A

Related

Command	Description

Commands	**show bgp ipv4 unicast dampening parameters**	Shows the IPv4 unicast route dampening parameters configured for BGP.

Platform Description N/A

show bgp ipv6 unicast neighbors

Use this command to show the related information of BGP IPv6 unicast neighbor.

show bgp ipv6 unicast neighbors *neighbor-address*

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 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	Shows the related information of BGP IPv4 unicast neighbor.

Platform Description N/A

show bgp ipv6 unicast paths

Use this command to show the path information of the IPv6 unicast in the route database.

show bgp ipv6 unicast 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

```
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	Shows the path information of the IPv4 unicast in the route database.

Platform Description N/A

show bgp ipv6 unicast summary

Use this command to show the related information of BGP IPv6 unicast.

show bgp ipv6 unicast summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to show 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	Shows the related information of BGP IPv4 unicast.

Platform Description N/A

show bgp vpnv4 unicast

Use this command to show 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	Shows neighbor information.
summary	Shows the route summary information.
label	Shows 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 Mode Privileged EXEC mode

Usage Guide This command is used to show the VPN information of all VRFs or RDs.

Configuration Examples

```
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 In the MPLS BGP application environment, bgp vrf routes are imported by routes prioritized by MP-BGP. Therefore, for the vpn route of the multi-route MP-BGP, the prioritized route is only displayed using the show bgp vpnv4 unicast vrf command. For the detailed MP-BGP route information, use the show bgp vpnv4 unicast all command.

show ip bgp

The function of the **show ip bgp** command is totally consistent with that of the **show bgp ipv4 unicast** command. All the parameters of the **show bgp ipv4 unicast** command can be used in the **show ip bgp** command.

Parameter Description	Parameter	Description
	Please refer to the detailed parameter description of the **show bgp ipv4 unicast** command.	Please refer to the detailed parameter description of the **show bgp ipv4 unicast** command.

Defaults Please refer to the detailed parameter description of the **show bgp ipv4 unicast** command.

Command Mode Privileged EXEC mode

Usage Guide Please refer to the detailed parameter description of the **show bgp ipv4 unicast** command.

Configuration Examples N/A

Related Commands	Command	Description
	show bgp ipv4 unicast	Shows IPv4 unicast routing information in the BGP routing information.

Platform Description N/A

show ip as-path-access-list

Use this command to show the related information of the AS path ACL.

show ip as-path-access-list [*num*|]

Parameter Description

Parameter	Description
num	as-path-access-list number to be displayed

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to view the as-path-access-list information.

Configuration Examples

```
Ruijie# show ip as-path-access-list
AS path access list 30
permit ^30s
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

IS-IS Commands

adjacency-check

Use this command to detect protocols supported by the adjacency in Hello packets. Use the **no** form of this command to cancel this detection.

adjacency-check

no adjacency-check

Parameter Description

Parameter	Description
-	-

Defaults The detection is enabled by default.

Command Mode IS-IS routing process configuration mode or address-family ipv6 mode

Usage Guide Protocols supported by adjacency are detected in Hello packets by default. Use the **no** form of this command to cancel the detection.

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
-	-

Platform Description N/A

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 254 characters at most
send-only	Specifies the plaintext authentication password of Level-1 area

	applicable to packets sent only, but not to packets received.

Defaults No authentication password is set by default.

Command Mode IS-IS routing process configuration mode

Usage Guide Configure this command to perform the authentication on LSP, CSPN and PSNP packets received in the Level-1 area and send packets together with the authentication information. In the same area, all IS-IS devices must be configured with the same password.
If the **authentication mode** command has been performed, this command cannot be configured. You need to cancel the **authentication mode** command first.
Running the **no area-password send-only** command can only disable the **send-only** option.

Configuration Examples Example 1: The following example specifies the authentication in the IS-IS area using the plaintext mode with the password of *redgiant* and the password is applicable to packets sent only, but not to the packets received.

```
Ruijie(config)# router isis
Ruijie(config-router)# area-password redgiant send-only
```

Related Commands

Command	Description
domain-password	Sets the Level-2 domain password.
authentication mode	Specifies the IS-IS authentication mode.

Platform Description N/A

authentication key-chain

Use this command to specify the key-chain used by the IS-IS authenticaiton. Use the **no** form of this command to cancel the key-chain specified.

authentication key-chain *name-of-chain* [**level-1 | level-2**]

no authentication key-chain *name-of-chain* [**level-1 | level-2**]

Parameter Description

Parameter	Description
name-of-chain	Key-chain name, with the maximum length of 255 characters
level-1	Specifies the authentication key-chain of the Level-1.
level-2	Specifies the authentication key-chain of the Level-2.

Defaults The authentication key-chain is not specified by default.

Command Mode IS-IS routing process configuration mode

Usage Guide

- If the **key chain** command is not used to configure the corresponding key-chain, the authentication will not be performed. In addition, to enable IS-IS key-chain authentication, you need to configure the **authentication mode** command at the same time.
- This key-chain can apply to plain-text authentication mode and MD5 encrypted authentication mode. You can use the **authentication mode** command to set the authentication mode.
- The password key-string in the key-chain must not exceed 254 characters if the plain-text authentication mode is used, otherwise this configuration will fail.
- Only one key-chain can be used at one time. So, when configuring this command, the original key-chain will be replaced by the specified new one.
- If no Level is specified, the key-chain will apply to both Level-1 and Level-2.
- The key-chain specified by this command applies to the LSP, CSNP and PSNP packets. IS-IS will send or receive the password that belongs to this key-chain.
- Key-chain may contain multiple passwords. When sending the packets, use the password with small number first. While receiving the packets, packets will be recieved as long as the password of this packet received corresponds to any password in the key-chain.

Configuration Examples

Example 1: 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	Specifies the IS-IS authentication mode.
authentication send-only	Specifies the IS-IS authentication applicable to sent packets only, but not to packets received.
key-chain	Configures the key-chain.

Platform Description

N/A

authentication mode

Use this command to specify the mode of IS-IS authentication. Use the **no** form of this command to cancel the specified IS-IS authentication mode.

authentication mode { **md5** | **text** } [**level-1** | **level-2**]

no authentication mode { **md5** | **text** } [**level-1** | **level-2**]

Parameter Description

Parameter	Description
md5	Specifies using MD5 authentication mode.
text	Specifies using plain-text authentication mode.
level-1	Specifies enabling authentication mode on Level-1.
level-2	Specifies enabling authentication mode on

	Level-2.

Default Configuration

The authentication mode is not specified by default.

Command Mode

IS-IS routing process configuration mode

Usage Guide

- To enable the key-chain configured by the **authentication key-chain** command, 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, the configured commands will be overwritten by the new command.
- If the **authentication mode** command has been configured, the **area-password** or **domain-password** cannot be configured. You need to delete the **authentication mode** command first.

Configuration Examples

Example 1: The following example specifies using MD5 authentication mode for authentication in the IS-IS area.

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication mode md5 level-1
```

Related Commands

Command	Description
area-password	Sets Area plaintext authentication password.
authentication key-chain	Specifies the key-chain used for IS-IS authenction.
authentication send-only	Specifies the IS-IS authentication applicable to packets sent only, but not to packets received.
domain-password	Sets the domain plaintext authenticaion password.

Platform Description

N/A

authentication send-only

Use this command to specify the IS-IS authentication only applicable to packets sent, but not to packets recieved. Use the **no** form of this command to cancel this mode, that is, to authenticate packets received.

authentication send-only [**level-1** | **level-2**]

no authentication send-only [**level-1** | **level-2**]

Parameter Description

Parameter	Description
level-1	Specifies setting **send-only** on the Level-1.

level-2	Specifies setting **send-only** on the Level-2.

Defaults

This command is not configured by default. If IS-IS authentication is configured, both sent and received packets will be authenticated.

Command mMode

IS-IS routing process configuration mode

Usage Guide

- With this command configured, IS-IS will set the authentication password in packets sent but received packets will not be authenticated. It applies to the following two situations: 1. before deploying IS-IS authentication for all devices in the network; 2. before changing the authentication password or authentication mode. Before starting the above two tasks, you need to configure the **authentication send-only** command to disable authentication on received packets to avoid network oscillation caused during the following authentication password deployment. After the deployment of the entire network authentication, use the **no isis authentication send-only** command to cancel the **send-only** authentication mode.
- This command applies to plain-text authentication mode and MD5 authentication mode. You can use the **authentication mode** command to set the authentication mode.
- If no Level is specified, the authentication mode specified is applicable to both Level-1 and Level-2.

Configuration Examples

Example 1: The following example specifies send-only as the authentication mode in the IS-IS area.

```
Ruijie(config)# router isis
Ruijie(config-router)# authentication send-only level-1
```

Related Commands

Command	Description
authentication key-chain	Specifies the IS-IS authentication key-chain.
authentication mode	Specifies the mode of IS-IS authentication.
key-chain	Configures the key-chain.

Platform Description

N/A

bfd all-interfaces

Use this command to perform link detection with BFD on all interfaces running the IS-IS protocol in IS-IS routing process configuration mode. Use the **no** form of this command to restore the default settings.

bfd all-interfaces [anti-congestion]

no bfd all-interfaces [anti-congestion]

Parameter Description

Parameter	Description
anti-congestion	Anti-congestion by running IS-IS with BFD on the interface

Defaults Disabled

Command mode IS-IS routing process configuration mode

Usage Guide There are two ways to enable or disable the cooperation with BFD on the interface running IS-IS:
First: use the [**no**] **bfd all-interfaces** [anti-congestion] command in IS-IS routing process configuration mode to enable or disable cooperation with BFD on all interfaces running IS-IS.
Second: use the **isis bfd** [**disable |** anti-congestion] command in interface configuration mode to enable or disable cooperation with BFD on the specified interface running IS-IS.
In normal cases, BFD send detecting packets to detect link state with intervals in milliseconds. When the link gets abnormal, for example, the link is disconnected, BFD can detect link anomaly quickly and inform IS-IS to delete neighbors and neighbors-reachable information in LSP packets. IS-IS performs routing calculation again to generate new a route, avoiding the abnormal link and achieving fast convergence, With the introduction of new technologies such as Multi-Service Transport Platform (MSTP), link is congestion-prone in peak periods of data communication. In congestion, BFD can detect link anomaly quickly and inform IS-IS to delete neighbors and neighbors-reachable information in LSP packets. Besides, BFD perform the link switch to avoid congestion. As the IS-IS neighbor detects that the interval to send Hello packets is 10s and the timeout period is 30s. When BFD detects anomaly, the router can receive IS-IS and establish IS-IS adjacency relation. The route restores to the congested link and performs BFD detection again. BFD repeats the process of detecting link anomaly and performing link switch, switching the route to either the congested link or other links and causing congestion.
Anti-congestion is enabled to avoid routing congestion caused by link congestion. Thus in link congestion, the IS-IS neighbor remains but the neighbor-reachable information is deleted in LSP packets. The route is switched to the non-congested link. After the link restores to normal, or rather non-congested, the neighbor-reachable information in LSP packets is restored and the route is switched back, avoiding routing congestion.
When IS-IS enables anti- congestion, both the **bfd all-interfaces** [**anti-congestion**] and the **bfd up-dampening** commands must be configured on the interface. Configuring only one command may cause ineffective anti- congestion or other network anomalies.
Refer to the examples in **isis bfd** command to learn how to enable BFD anti-congestion on the interface.

The BFD session needs to be set on the interface before configuring IS-IS with BFD.

When the interface is configured with the **bfd up-dampening** command, the **bfd all-interfaces** [**anti-congestion**] command must be enabled if IS-IS is used with BFD on the interface.

The **bfd all-interfaces** [**anti-congestion**] command must be configured together with

the **bfd up-dampening** command on the interface.

Configuration Examples

```
Ruijie(config)# router isis 123
Ruijie(config-router)# bfd all-interface
```

Related Commands

Command	Description
bfd	Configures BFD session parameters.
isis bfd [**disable** | anti-congestion]	Enables the specified interface running IS-IS or disables link detection with BFD
show isis interface	Displays the interface running IS-IS.
show isis neighbors detail	Displays the neighbors running IS-IS.
show bfd neighbors detail	Displays the BDF session.
bfd up-dampening	Configures the UP status duration before advertising the UP status to the associated application session.

Platform Description N/A

clear clns neighbors

Use this command to clear all IS-IS neighbor relation tables.

clear clns neighbors

Parameter Description

Parameter	Description
-	-

Defaults No IS-IS neighbor relation table is deleted by default.

Command Mode Privileged EXEC mode

Usage Guide This command is used when it needs to refresh the IS-IS neighbor relation table immediately.

Configuration Examples

```
Ruijie# clear clns neighbors
```

Related Commands

Command	Description
clear isis	Clears all IS-IS data structure.

Platform Description N/A

clear isis *

Use this command to clear data structures of all IS-ISs.

clear isis *

Parameter Description

Parameter	Description
-	-

Defaults No IS-IS data structure is not deleted by default.

Command Mode Privileged EXEC mode

Usage Guide This command is used when it needs to refresh LSP immediately. For example, after executing the **area-password** and **domain-password** commands, previous LSPs still exist in this device, you can use this command to clear these LSPs.

Configuration Examples

```
Ruijie# clear isis *
```

Related Commands

Command	Description
clear clns neighbors	Clears all IS-IS neighbors.

Platform Description N/A

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 No statistic of IS-IS is deleted by default.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# clear isis counter
```

Related

Command	Description

commands	clear isis *	Clears data structures of all IS-ISs.

Platform Description N/A

default-information originate

Use this command to generate a default routing information and distribute it through 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

Parameter Description

Parameter	Description
map-name	(Optional) Associated route-map's name, with a maximum length of 32 characters, no route-map is associated by default

Defaults No default route is generated by default.

Command Mode IS-IS routing process configuration mode or address-family ipv6 mode

Usage Guide No default route is generated in Level-2 domain. Use this command to allow the default route to enter 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
-	-

Platform Description N/A

distance

Use this command to set the management distance of the IS-IS routes. Use the **no** form of this command to restore the default value.

distance ***my-cost***

no distance

Parameter Description	Parameter	Description
	my-cost	Distance value, in the range from 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 is, the more reliable the routing information is.

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# distance 100
```

Related Commands	Command	Description
	isis metric	Sets the metric value of the interface.

Platform Description N/A

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 a max length of 254 characters
	send-only	Specifies the plain-text authentication password of the Level-2 domain applicable to packets sent only, but not to packets received.

Defaults No authentication password is set by default.

Command Mode IS-IS routing process configuration mode

Usage Guide Configure this command to authenticate LSP, CSPN and PSNP packets received in the Level-2 domain and send packets together with the authentication information. In the Level-2 domain, all IS-IS devices must be configured with the same password.
If the **authentication mode** command has been executed, this command cannot be configured. 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	Sets the plain-text authentication password of Level-1 area.
authentication mode	Specifies the IS-IS authentication mode.

Platform Description N/A

enable traps

IS-IS supports 18 types of TRAP packets. Use this command to allow all one or several types of packets to be sent. Use the **no** form of this command to disable it.
enable traps { **all** | *traps set* }
no enable traps { **all** | *traps set* }

Parameter Description

Parameter	Description
All	All IS-IS TRAP packets
traps set	Specifies one type of IS-IS TRAP packet in any set.

Defaults Disabled

Command mode IS-IS routing process configuration mode

Usage Guide There are 18 types of IS-IS packets. Based on different features, they are divided into several sets and each set includes several types of IS-IS TRAP packets. Enable IS-IS TRAP globally in global configuration mode (with the **snmp-server enable traps isis** command), specify the host receiving TRAP packets, and use this command to specify the types of IS-IS TRAP packets allowed to be sent in IS-IS routing process configuration mode. Then IS-IS packets can be transmitted.

Configuration Examples The following example allows all IS-IS TRAP packets to be sent to host 10.1.1.1.

```
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
snmp-server enable traps isis	Enables IS-IS TRAP globally

Platform Description N/A

exit-address-family

Use this command to exit IS-IS address-family ipv6 configuration mode and returns 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 shows how to exit IS-IS address-family ipv6 configuration mode

```
Ruijie (config-router-af)#exit-address-family
Ruijie (config-router)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

graceful-restart

Use this command to enable IS-IS GR Restart. Use the **no** form of this command to disable it.

graceful-restart

no graceful-restart

Parameter Description

Parameter	Description
N/A	-

Defaults IS-IS GR Restart is disabled by default.

Command Mode IS-IS routing process configuration mode

Usage Guide

With this command used, after the device restarts, the IS-IS protocol state can be restored to the state before restart without affecting data forwarding if the network status remains the same.

With IS-IS GR Restart enabled on the device of multiple management boards, the holdtime for maintaining the IS-IS adjacent relation must not be less than 40 seconds to ensure IS-IS graceful restart when the management boards are switched over suddenly. You can configure the holdtime using the **isis hello-interval** and **isis hello-multiplier** commands. When the holdtime is less than 40s, the holdtime in the Hello packet header will be set to 40 seconds by default.


Note

The IS-IS device needs the help of the GR Helper neighbor device to perform graceful-restart.

Configuration Examples

Example 1: The following example enables IS-IS GR Restart.

```
Ruijie(config)# router isis
Ruijie(config-router)# graceful-restart
```

Related Commands

Command	Description
graceful-restart helper disable	Disables IS-IS GR Help.
isis hello-interval	Sets the interval of sending Hello packets.
isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.

Platform Description IS-IS GR Restart is now supported on the platform supporting the standby hot environment only, such as S8600 series.

graceful-restart grace-period

Use this command to configure the maximal interval for graceful-restart. Use the **no** form of this command to restore the default value.

graceful-restart grace-period *seconds*

no graceful-restart grace-period

Parameter Description	Parameter	Description
	second	Time interval allowed for device graceful-restart, in the range of 1 to 65535 seconds

Defaults The default value is 300s.

Command Mode IS-IS routing process configuration mode

Usage Guide N/A

Configuration Examples Example 1: The following example sets the interval of grace-restart to 40s.

```
Ruijie(config)# router isis
Ruijie(config-router)# graceful-restart grace-period 40
```

Related Commands	Command	Description
	graceful-restart	Enables IS-IS GR Restart.
	show isis graceful-restart	Shows the status information of IS-IS GR Restart.

Platform Description N/A

graceful-restart helper disable

Use this command to disable IS-IS GR Help. Use the **no** form of this command to enable it.

graceful-restart helper disable

no graceful-restart helper disable

Parameter Description	Parameter	Description
	N/A	-

Defaults IS-IS GR Help is enabled by default.

Command Mode IS-IS routing process configuration mode

Usage Guide Use the command to disable IS-IS GR Help. In this case, the IS-IS will ignore the request of graceful-restarting the device.

Configuration Examples Example 1: The following example disables IS-IS GR Help.

```
Ruijie(config)# router isis
```

```
Ruijie(config-router)# graceful-restart helper disable
```

Related Command	Command	Description
	graceful-restart	Enables IS-IS GR Restart.

Platform Description N/A

hello padding

Use this command to pad IS-IS Hello packets. Use the **no** form of this command and no IS-IS Hello packet will be padded.

hello padding [**multi-point | point-to-point**]

no hello padding [**multi-point | point-to-point**]

Parameter Description	Parameter	Description
	multi-point	Pads LAN Hello packets.
	point-to-point	Pads P2P Hello packets.

Defaults LAN and P2P Hello packets are padded by default.

Command Mode IS-IS route process configuration mode

Usage Guide By padding Hello packets, adjacency can be notified of MTU supported by the device. Use the command to set the padding mode for all Hello packets sent by the IS-IS process. You can set padding mode for LAN and P2P Hello packets separately, for example, not to pad LAN or P2P Hello packets.
A corresponding **isis hello padding** command is provided under the interface mode. As long as padding for the Hello packets is cancelled in IS-IS route process configuration mode, or padding for Hello packets sent by the interface is cancelled in interface configuration mode, all Hello packets sent by the interface will not be padded.

Configuration Examples Example 1: The following example cancels padding for P2P Hello packets.

```
Ruijie(config)# router isis
Ruijie(config-router)# no hello padding point-to-point
```

Related Commands	Command	Description
	isis hello-padding	Pads IS-IS Hello packets sent on the interface.

Platform Description N/A

hostname dynamic

Use this command to repalce the System ID of the router with the destination node's hostname. Use the **no** form of this command to cancel this replacement.

hostname dynamic

no hostname dynamic

Parameter Description	**Parameter**	**Description**
	-	-

Defaults The hostname dynamic function is enabled by default.

Command Mode IS-IS routing process configuration mode

Usage Guide With this command configured, the hostname of the destination node replaces the System ID. The System ID shown with the command such as **show isis database, show isis neighbors** is replaced by the hostname of the destination node.

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# hostname dynamic
```

Related Commands	**Command**	**Description**
	-	-

Platform Description N/A

ignore-lsp-errors

Use this command to ignore the LSP checksum and checksum errors. Use the **no** form of this command not to ignore the LSP checksum and errors.

ignore-lsp-errors

no ignore-lsp-errors

Parameter Description	**Parameter**	**Description**
	-	-

Defaults LSP checksum and errors are not ignored by default.

Command Mode IS-IS routing process configuration mode

Usage Guide When the local IS-IS receives a LSP, it will examine and calculate the LSP 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 use the ignore-lsp-errors command to ignore the checksum errors, LSP packets with wrong checksum will be processed as normal packets.

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# ignore-lsp-errors
```

Related Commands

Command	Description
-	-

Platform Description

N/A

ip router isis

Use this command to support IPv4 IS-IS on the specified interface. The **no** form of this command disables 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 Ipv4 IS-IS is disabled on the interface by default.

Command Mode Interface configuration mode

Usage Guide

Configure this command to enable IS-IS IPv4 routing protocol on the interface. The no form of this command disables IS-IS IPv4 routing.

If no ip routing is executed in global configuration mode, the IS-IS will disable IS-IS 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.

In order to avoid routing blackholes on the network where IPv4 and IPv6 coexist, if protocols supported by two devices or interfaces are not the same, adjacency relation will not be set up. In this case, please check whether the network topology has any problem. If there is no problem with the network topology and there are no routing blackholes, configure different instances to perform IPv4 and IPv6 routes learning.

Configuration Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip router isis
```

Related Commands

Command	Description
ipv6 router isis	Enables IPv6 IS-IS on the interface.
router isis	Creates IS-IS instances.

Platform Description N/A

Ipv6 router isis

Use this command to support IPv6 IS-IS on the specified interface. The **no** form of this command disables 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 Ipv6 IS-IS is disabled on the interface by default.

Command Mode Interface configuration mode

Usage Guide Configure this command to enable IS-IS IPv6 routing protocol on the interface. If **no ipv6 unicast-routing** is executed in global configuration mode, the IS-IS will disable IS-IS IPv6 routing function on all interfaces, while other IS-IS configurations will remain unchanged.
In order to avoid the routing blackhole on the network where IPv4 and IPv6 coexist, if protocols supported by two devices or interfaces are not the same, adjacency relation will not be established. In this case, please check whether the network topology has any problem. If there is no problem with the network topology and there is no routing blackhole, use different configuration examples to learn IPv4 and IPv6 routing.

Configuration Examples

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ipv6 router isis
```

Related Commands

Command	Description
ip router isis	Enables IPv4 IS-IS on the interface.
router isis	Creates IS-IS instances.

Platform Description N/A

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 specifed 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 a maximum length of 255 characters
level-1	Specifies the authentication key-chain of Level-1.
level-2	Specifies the authentication key-chain of Level-2.

Defaults No IS-IS interface authentication key-chain is specified by default.

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 enable the IS-IS key-chain authentication, 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 password key-string in the key-chain must not exceed 254 characters if the plain-text authentication mode is used, otherwise this configuration will fail.
- Only one key-chain is used at one time. Therefore, when configuring this command, the original key-chain will be overwritten by the specified new one.
- If 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 Hello packets. IS-IS will send or receive the password that belongs to this key-chain.
- The key-chain may contain multiple passwords. When sending packets, use the password with small number first. While receiving the packets, packets will be recieved as long as the password of this packet received corresponds to any password in the key-chain.
- The authentication commands configured in 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

Example 1: 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

Command	Description

Commands		
	isis authentication mode	Specifies the mode of IS-IS interface authentication.
	isis authentication send-only	Specifies IS-IS interface authentication only applicable to packets sent, but not to packets received.
	key-chain	Configures the key-chain.

Platform Description N/A

isis authentication mode

Use this command to specify the IS-IS interface authentication mode. 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	Specifies the MD5 authentication mode.
text	Specifies the plain-text authentication mode.
level-1	Specifies the interface authentication mode to take effect on Level-1.
level-2	Specifies the interface authentication mode to take effect on Level-2.

Defaults No interface authentication mode is specified by default.

Command Mode Interface configuration mode

Usage Guideline

- 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 authenticatin 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, isis password cannot be configured. Therefore, you need to delete the **isis authentication mode** command first.

Configuration Examples

Example 1: The following example specifies MD5 authentication mode as the authentication mode on Level-2 of the interface GigabitEthernet 0/1.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis authentication mode md5 level-2
```

Related

Command	Description

Commands		
	isis authentication key-chain	Specifies the key-chain used by the IS-IS interface authentication.
	isis authentication send-only	Specifies the IS-IS interface authentication to only apply on packets sent, but not on packets received.
	key-chain	Configures the key-chain.
	isis password	Sets the plain-text authentication password for the packets transmit on the IS-IS interface.

Platform Description N/A

isis authentication send-only

Use this command to specify the IS-IS interface authentication to only apply to packets sent and not to packets recieved. The **no** form of this command cancels this authenticaiton mode, that is, restore the authetication 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	Sets send-only on Level-1 of the interface.
level-2	Sets send-only on Level-2 of the interface.

Defaults This command is not configured by default. If IS-IS interface authentication has been configured, then the authentication will be performed on packets sent and received.

Command Mode Interface configuration mode

Usage Guide

- With this command configured, IS-IS will set the authentication password in Hello packets sent from the interface, however, the authentication will not be performed on Hello packets received. It can apply to the following two situations: 1. before deploying IS-IS interface authentication for all devices in the network. 2. before changing the authentication password or authentication mode. Before starting the above two tasks, you need to configure isis **authentication send-only** command first to disable authentication on Hello packets received to avoid network oscillation caused during the following IS-IS interface authentication deployment. After the deployment of the entire network authentication, execute the **no isis authentication send-only** command to cancel 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 IS-IS interface authentication.
- If Level is not specified, the authentication mode specified is applicable to Level-1 and Level-2.

Configuration Example 1: The following example specifies the authentication on Level-1 of the interface

Examples GigabitEthernet 0/1 using send-only authentication mode.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis authentication send-only level-1
```

Related Commands

Command	Description
isis authentication key-chain	Specifies the key-chain used by IS-IS interface authentication.
isis authentication mode	Specifies the mode of IS-IS interface authentication.
key-chain	Configures the key-chain.

Platform Description N/A

isis bfd

Use this command to enable IS-IS to cooperate with BFD. Use the no form of this command to cancel the setting.

isis bfd [**disable** | anti-congestion]

no isis bfd [**disable** | anti-congestion]

Parameter Description

Parameter	Description
disable	Cancels linkage between IS-IS and BFD on the interface.
anti-congestion	Anti-congestion by by running IS-IS with BFD on the interface

Defaults If **bfd all-interfaces** command is executed, correlation between IS-IS and BFD is enabled by interfaces running IS-IS by default.

If **bfd all-interfaces** command is not executed, correlation between IS-IS and BFD is disabled by interfaces running IS-IS by default. Anti-congestion function is disabled by default.

Command mode Interface configuration mode

Usage Guide There are two ways to enable or disable the cooperation with BFD on the interface running IS-IS:

First: use the [**no**] **bfd all-interfaces** [anti-congestion] command in IS-IS routing process configuration mode to enable or disable cooperation with BFD on all interfaces running IS-IS.

Second: use the **isis bfd** [**disable |** anti-congestion] command in interface configuration mode to enable or disable cooperation with BFD on the specified interface running IS-IS.

In normal cases, BFD send detecting packets to detect link state with intervals in milliseconds. When the link gets abnormal, for example, the link is disconnected, BFD can detect link anomaly quickly and inform IS-IS to delete neighbors and neighbors-reachable information in LSP packets. IS-IS performs routing calculation again to generate new a route, avoiding the abnormal link and achieving fast convergence, With the introduction of new technologies such as Multi-Service Transport Platform (MSTP), link is congestion-prone in peak periods of data communication. In congestion, BFD can

detect link anomaly quickly and inform IS-IS to delete neighbors and neighbors-reachable information in LSP packets. Besides, BFD perform the link switch to avoid congestion. As the IS-IS neighbor detects that the interval to send Hello packets is 10s and the timeout period is 30s. When BFD detects anomaly, the router can receive IS-IS and establish IS-IS adjacency relation. The route restores to the congested link and performs BFD detection again. BFD repeats the process of detecting link anomaly and performing link switch, switching the route to either the congested link or other links and causing congestion.

Anti-congestion is enabled to avoid routing congestion caused by link congestion. Thus in link congestion, the IS-IS neighbor remains but the neighbor-reachable information is deleted in LSP packets. The route is switched to the non-congested link. After the link restores to normal, or rather non-congested, the neighbor-reachable information in LSP packets is restored and the route is switched back, avoiding routing congestion.

When IS-IS enables anti-congestion, both the **bfd all-interfaces** [**anti-congestion**] and the **bfd up-dampening** commands must be configured on the interface. Configuring only one command may cause ineffective anti-congestion or other network anomalies.


Caution The BFD session needs to be set on the interface before configuring IS-IS with BFD.

Configuration Examples

The following example shows how to cancel the correlation between IS-IS and BFD on interface FastEthernet 0/1.

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# isis bfd disable
```

The following example configures the **bfd up-dampening** command on the interface FastEthernet 0/1 to enable anti-congestion by IS-IS with BFD.

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# no switchport
Ruijie(config-if)# isis bfd anti-congestion
Ruijie(config-if)# bfd up-dampening 60000
```

Related Commands

Command	Description
bfd	Configures BFD session parameters.
bfd all-interfaces [anti-congestion]	Enables all interface routing protocols to cooperate with BFD.
show isis interface	Displays information of the interface running IS-IS
show isis neighbors detail	Displays IS-IS neighbors information.
show bfd neighbors detail	Displays BFD session information.
bfd up-dampening	Configures the UP status duration before advertising the UP status to the associated application session.

Platform N/A

Description

isis circuit-type

Use this command to set the circuit-type for the IS-IS interface. The **no** form of this command restores the default setting.

isis circuit-type {**level-1 | level-1-2 | level-2-only**}

no isis circuit-type

Parameter Description

Parameter	Description
level-1	Forms Level-1 adjacency.
leve-2-only	Forms Level-2 adjacency.
level-1-2	Forms Level-1-2 adjacency.

Defaults The circuit-type is Level-1-2 by default.

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 as 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	Sets Level of IS-IS instance.

Platform Description N/A

isis csnp-interval

Use this command to set the interval (in second) for broadcasting CSNP packets on IS-IS interface. The **no** form of this command can restore 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 CSNP packets in the range of 0 to 65535 seconds.

level-1	Interval for sending CSNP packets configured only on Level-1.
level-2	Interval for sending CSNP packets configured only on Level-2.

Default

By default, in the broadcast network, the interval for sending CSNP packets is 10 seconds. While in P2P interface network, no CSNP packet is sent by default.
When using this command without parameter Level-1 and Level-2, the new setting is applicable to the Level-1 and Level-2 at the time by default.

Command Mode

Interface configuration mode

Usage Guide

Configure this command to change the interval for sending CSNP packets. By default, the DIS on the broadcast network sends CSNP packets at an interval of 10s.
For P2P interface network, CSNP packets will only be sent at the beginning of adjacency formation by default. If the interface is set to mesh-groups, you can configure to send CSNP packetsperiodically.
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
-	-

Platform Description

N/A

isis hello-interval

Use this command to set the interval (in second) for sending Hello packets on the interface. The **no** form of this command restores 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 Hello packet, in the range of 1 to 65535 seconds
minimal	Sets holdtime to the minimal value of 1.
level-1	Sets Level to Level-1.
level-2	Sets Level to Level-2.

Defaults

By default, the interval is 10 seconds, which is applicable to both Level-1 and Level-2.

When using this command without parameter Level-1 and Level-2, the new setting is applicable to both Level-1 and Level-2 by default.

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 on IS-IS interface is 3, and DIS in broadcast network sends Hello packets at an interval that is three times of non-DIS. If this IS is elected as DIS on this interface, the interface will send Hello a packet every 3.3 seconds by default.
If the key word "minimal" is used, then the "holdtime" in Hello packets is 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 will be 1/4s (250ms). By default, 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	Sets the multiplier of the Hello holdtime.

Platform Description N/A

isis hello-multiplier

Use this command to set the multiplier of Hello holdtime. The **no** form of this command restores the default value.

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, in the range of 2 to 100.

Defaults The multiplier is 3 by default.

Command Mode	IS-IS routing process configuration mode
Usage Guide	Use this command to set the multiplier of Hello holdtime. The holdtime value in Hello packets is the product of multiplying 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	Sets the interval for sending Hello packets.

Platform Description	N/A

isis hello padding

Use this command to pad IS-IS Hello packets sent on IS-IS interface. The **no** form of this command is used to not pad the IS-IS Hello packets.

isis hello padding

no isis hello padding

Parameter Description

Parameter	Description
-	-

Default	Hello packets sent on the interface are padded by default.
Command Mode	Interface configuration mode
Usage Guide	Pad IS-IS Hello packets to advertise the MTU supported to the neighbors. A corresponding **hello padding** command is provided in IS-IS route process configuration mode. As long as padding for the Hello packets is cancelled in IS-IS route process configuration mode, or padding for Hello packets sent by the interface is cancelled in interface configuration mode, all Hello packets sent by the interface will not be padded.

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	Sets the interval for sending Hello packets.
hello padding	Sets the padding way for Hello packets.

Platform Description N/A

isis lsp-interval

Use this command to set the interval for the LSP PDU transmission on IS-IS interface. The **no** form of this command can restore the default value.

isis lsp-interval *interval*

no isis lsp-interval

Parameter Description

Parameter	Description
interval	Interval time, in the range of 1 to 4294967295 milliseconds.

Default The lsp-interval is 33ms by default.

Command Mode Interface configuration mode

Usage Guide This command is used to set the minimal interval for sending LSPs on the interface, with the unit of 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	Sets the LSP retransmission interval in the P2P network.

Platform Description N/A

isis mesh-group

Use this command to add the IS-IS interface to the specified mesh-group. The **no** form of this command is used to remove the interface from the mesh-group.

isis mesh-group { **blocked |** *mesh-group-id* }

no isis mesh-group

Parameter Description

Parameter	Description
blocked	Blocks all LSP forwarding on the interface.
mesh-group-id	Adds the interface to the mesh-group of specified

	mesh-group-id with the range of 1 to 4294967295.

Defaults The interface is not added to any mesh-group by default.

Command Mode Interface configuration mode

Usage Guide Mesh-groups can control the transitional and redundant LSP spreading in the NBMA network. In the normal condition, the IS-IS node spreads out the LSP from all interfaces except for the receiving one, that is, if a router is configured with multiple subintefaces, the LSP will be sent from all subinterfaces and the neighbors will receive multiple LSPs, causing huge waste of CPU and bandwidth. The IS-IS mesh-group allows grouping the interfaces of the routing device. When 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 routing device recieves 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	Sets Point-to-Point as the Broadcast interface type of IS-IS.

Platform Description N/A

isis metric

Use this command to set the metric value for the interface. The **no** form of this command restores the 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	Sets this metric to apply on Level-1 circuit.
level-2	Sets this metric to apply on Level-2 circuit.

Defaults The metric is 10 by default, applicable on both Level-1 and Level-2 circuit.

Command Mode Interface configuration mode

Usage Guide The Metric value is in TLV of the IP reachable information and is applied to 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	Sets the metric type.
isis wide-metric	Sets the wide metric of the IS-IS interface.

Platform Description N/A

isis network point-to-point

Use this command to set Point-to-Point as the IS-IS Broadcast interface 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
point-point	Point-to-point network

Defaults The **isis network point-point** is not executed by default.

Command Mode Interface configuration mode

Usage Guide This command is used to set the IS-IS Broadcast interface to Point-to-Point. This command applies to Broadcast interface only.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis network point-to-point
```

Related

Command	Description

Commands		
	isis mesh-group	Adds the IS-IS interface into the specified mesh group.

Platform Description N/A

isis password

Use this command to set the plain-text authentication password for Hello packets on the interface. The **no** form of this command cancels the password.

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 of 254 characters.
send-only	The plain-text authentication password is only applicable to packets sent. Received packets will not be authenticated.
level-1	This password applies to Level-1 circuit.
level-2	This password applies to Level-2 circuit.

Defaults By default, Level-1 and Level-2 are not configured with password.

Command Mode Interface configuration mode

Usage Guide

This command is used to set the plain-text authentication password for Hello packets ton the interface. Use the no form of this command to delete the passwords. When 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 cannot be configured. To configure this command, you need to delete the i**sis authentication mode** command first.
The no isis password **send-only** command can only be used to 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	Specifies the IS-IS interface authentication mode.

Platform Description N/A

isis priority

Use this command to set the priority for the DIS election on LAN. The **no** form of this command restores the default priority.

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	Applies the priority on Level-1 circuit.
level-2	Applies the priority on Level-2 circuit.

Defaults The default priority value is 4 and is applied on both Level-1 and Level-2 circuit.

Command Mode Interface configuration mode

Usage Guide

Use this command to change the priority value in Hello packets of LAN.
Packets with low priority value has a lower priority in DIS election than those with low priority value.
This command takes no effect on Point-to-Point network interface.
The **no isis priority** command is used to restore the default priority value no matter whether the command is followed by a parameter. 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 default priority value.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis priority 127 level-1
```

Related Commands

Command	Description
-	-

Platform Description N/A

isis psnp-interval

Use this command to set the minimal interval to send PSNP packets. Use the **no** form of this command as the default setting.
isis psnp-interval seconds [**level-1** | **level-2**]
no isis psnp-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description

seconds	Within the range from 1 to 120s.
level-1	Functions only on Level-1.
level-2	Functions only on Level-2.

Defaults This command is not executed by default with the minimal interval of 2s and functions on both Level-1 and Level-2.

Command mode Interface configuration mode

Usage Guide PSNP packets are mainly used to ask for the LSP packets that are not in the local database or confirm received LSP packets (for a point-to-point network). In both cases, the faster PSNP packets are sent, the better. If there are many LSP packets while the device performance is relatively poor, it is suggested to prolong PSNP packets sending interval and LSP retransmission interval.

Configuration Examples The following example shows how to set the time interval to send Level-2 PSNP packets on interface GigabitEthernet 0/1 as 5s.

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# isis psnp-interval 5  level-2
```

Related Commands

Command	Description
isis retransmit-interval	The time interval to retransmit LSP.

Platform Description N/A

isis retransmit-interval

Use this command to set the LSP packets retransmission interval on IS-IS interface. The **no** form of this command restores the default interval.

isis retransmit-interval seconds [**level-1** | **level-2**]

no isis retransmit-interval [**level-1** | **level-2**]

Parameter Description

Parameter	Description
seconds	Time interval within the range from 0 to 65535s
level-1	Functions only on Level-1.
level-2	Function only on Level-2.

Defaults If this command is not executed by default, retransmit-interval is 5s.

If the level is not specified, the command functions on both Level-1 and Level-2.

Command mode Interface configuration mode

Usage Guide This command is used to set the LSP packets 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 LSP packets in the retransmit-interval, it will retransmit LSP packets.

Configuration Examples The following example shows how to set Level-2 LSP retransmission interval on interface serial 0/1 as 10s.

```
Ruijie# configure terminal
Ruijie(config)# interface serial 0/1
Ruijie(config-if)# isis retransmit-interval 10
```

Related Commands

Command	Description
isis lsp-interval	Interval for publishing LSP on the interface

Platform Description N/A

isis three-way-handshake disable

Use this command to cancel three-way-handshake negotiation on a point-to-point link in interface configuration mode. Use the **no** form of this command to restore the setting.
isis three-way-handshake disable
no isis three-way-handshake disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Enabled

Command mode Interface configuration mode

Usage Guide By default, IS-IS needs to perform three-way-handshake negotiation to establish point-to-point adjacency relation on a point-to-point link. Point-to-point adjacency relation is established only if three-way-handshake negotiation is successful. This command is used to cancel three-way-handshake negotiation in some cases, for example, adjacency formation needs to be sped up or the device does not support three-way-handshake negotiation.

Configuration Examples The following example shows how to cancel three-way-handshake negotiation on interface FastEthernet 0/0.

```
Ruijie# configure terminal
```

```
Ruijie(config)#
R11(config)#int fastEthernet 0/0
R11(config-if-FastEthernet 0/0)# isis network point-to-point
R11(config-if-FastEthernet 0/0)# isis three-way-handshake disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

isis wide-metric

Use this command to set the wide metric of IS-IS interface. The **no** form of this command is used to restore 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	Sets this Metric to apply on Level-1 circuit.
level-2	Sets this Metric to apply on Level-2 circuit.

Defaults The metric value is 10 by default and is applicable to both Level-1 and Level-2 circuit.

Command Mode Interface configuration mode

Usage Guide The Metric value is in 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	Sets the Metric type.
isis metric	Sets the Metric value of IS-IS interface.

Platform N/A

Description

is-type

Use this command to specify the level run by ISIS. The **no** form of this command is used to restore the default setting.

is-type { **level-1 | level-1-2 | level-2-only** }

no is-type

Parameter Description

Parameter	Description
level-1	Specifies IS-IS running on Level-1 only.
level-1-2	Specifies IS-IS running on both Level-1 and Level-2.
level-2-only	Specifies IS-IS running on Level-2 only.

Defaults

By default, if there is no IS-IS instance of Level-2 (including Level-1-2), is-type is Level-1-2.
Besides, if there is IS-IS instance running on the Level-2 (including Level-1-2), is-type is Level-1.

Command Mode

IS-IS routing process configuration mode

Usage Guide

Changing is-type will enable or disable the route of one Level.
There is only one instance running on the Level-2 (including Level-1-1) on a device.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# is-type level-1
```

Related Commands

Command	Description
isis circuit-type	Sets the IS-IS circuit type of the interface.

Platform Description

N/A

log-adjacency-changes

Use this command to log changes of the IS adjacency status when debug is disabled. The **no** form of this command disables this function.

log- adjacency -changes

no log- adjacency –changes

Parameter Description

Parameter	Description
-	-

Defaults

This function is enabled by default.

Command Mode	IS-IS routing process configuration mode
Usage Guide	You can also use the **debug** command to log changes of the IS adjacency status. But using the IS-IS's **debug** command will exhaust large numbers of resources.
Configuration Examples	`Ruijie(config-router)# log-adjacency-changes`

Related Commands

Command	Description
-	-

Platform Description	N/A

lsp-fragments-extend

Use this command to enable fragments extension function in IS-IS routing process configuration mode. Use the **no** form of this command to disable the function.
lsp-fragments-extend [**level-1 | level-2**] [**compatible rfc3786**]
no lsp-fragments-extend [**level-1** | **level-2**] [**compatible rfc3786**]

Parameter Description

Parameter	Description
level-1	Enables lsp extension function only on Level-1.
level-2	Enables lsp extension function only on Level-2.
compatible	Compatible with the RFC version to extend LSP.
rfc3786	The old version to extend LSP.

Defaults	The fragments extension function is disabled by default. If the level is not specified, the fragments extension function is enabled on both Level-1 and Level-2 by default. The standard supported by default is the latest RFC5311 version.
Command mode	IS-IS routing process configuration mode
Usage Guide	The original LSP packet has up to 256 fragments. After they are filled, the subsequent link state information includes neighbor information and IP routing information will be discarded directly, causing network anomaly. This problem can be avoided by enabling fragments extension. .Use this command to enable fragments extension on the specified level and use the **virtual-system** command to set additional system ID. Then the fragments extension function is enabled. If there are other devices supporting old RFC 3786 from other manufacturers, configure the “compatible” option. Pay attention to the link state database of the device when the “compatible”

option is enabled or disabled. If there are LSP packet residues affecting network routes, execute the clear isis * command to clear the LSP packet residues, triggering timely synchronization of the link state database.

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# lsp-fragments-extend level-2
```

Related Commands

Command	Description
virtual-system	Configures additional system ID.

Platform Description N/A

lsp-gen-interval

Use this command to set the minimal interval of the LSP generation. The **no** form of this command can restore the default value.

lsp-gen-interval [**level-1 | level-2**] *value*

no lsp-gen-interval

Parameter Description

Parameter	Description
value	The minimal interval of the LSP generation within the range from 1 to 120 seconds.
level-1	The minimal interval is applicable on Level-1 IS-IS.
level-2	The minimal interval is applicable on Level-2 IS-IS.

Defaults By default, this command is not configured and the interval of the minimal generation is 5s, 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 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 refreshing interval

Platform Description N/A

lsp-length originate

Use this command to set the maximal length of LSP packets to be sent in IS-IS routing process configuration mode. Use the **no** form of this command to restore the maximal length to the default value.

lsp-length originate *size* [**level-1** | **level-2**]

no lsp-length originate [**level-1** | **level-2**]

Parameter Description	Parameter	Description
	size	The maximal length of LAP packets to be sent within the range from 512 to 16000 bytes.
	level-1	Functions only on Level-1.
	level-2	Functions only on level-2.

Defaults 1492. If the level is not specified, this command functions on both Level-1 and Level-2 by default.

Command mode IS-IS routing process configuration mode

Usage Guide In principle, the LSP packet cannot be greater than the interface MTU in length. Otherwise, the LSP packet will be discarded directly when it is sent.

Configuration Examples The following example shows how to set the maximal length of a LS LSP packet as 1498 bytes.

```
Ruijie# configure terminal
Ruijie(config)# router isis 1
Ruijie(config-router)# lsp-length originate 1498 level-2
```

Related Commands	Command	Description
	lsp-length receive	The maximal length of LSP packets to be received.

Platform Description N/A

lsp-refresh-interval

Use this command to set the LSP refresh interval. The **no** form of this command restores 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 seconds.

Defaults The lsp-refresh-interval is 900 seconds by default.

Command Mode IS-IS routing process configuration mode

Usage Guide if the LSP remains stable during 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
-	-

Platform Description N/A

max-area-addresses

Use this command to set the maximal number of area addresses. The **no** form of this command restores the default value.

max-area-addresses *value*

no max-area-addresses

Parameter Description

Parameter	Description
value	The maximal number of area addresses allowed, in the range of 3 to 6

Defaults By default, max-area-addreses is 3.

Command Mode	IS-IS routing process configuration mode
Usage Guide	For the IS nodes of Level-1, only those with the same max-area-addresses can 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	Sets the IS-IS NET (Network Entry Title) address.

Platform Description	N/A

max-lsp-lifetime

Use this command to set the maximum value of the LSP lifetime. The **no** form of this command restores the default value.

max-lsp-lifetime *value*

no max-lsp-lifetime

Parameter Description

Parameter	Description
value	Maximum LSP lifetime, in the range of 1 to 65535 seconds.

Defaults	The max-lsp-lifetime is 1200 seconds by default.
Command Mode	IS-IS routing process configuration mode
Usage Guide	It should be noted that max-lsp-lifetime must be greater 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

metric-style

Use this command to set the metric style. The **no** form of this command restores 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	Adopts the old metric style with the router interface metric ranging from 1 to 63.
wide	Adopts the new metric style with the router interface metric ranging from 1 to 16777214
transition	Allows the routing device to send and receive the new and old metric style.
level-1	This metric-style applies 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 The metric-style is narrow by default.

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* when the metric-style is set to wide or **transiton.**

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie(config-router)# metric-style wide
```

Related Commands

Command	Description
isis metric	Sets the metric of the IS-IS interface.
isis wide-metric	Sets the wide metric of the IS-IS interface.

Platform Description N/A

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

No NET address is set by default.

Command Mode

IS-IS routing process configuration mode

Usage Guide

This command is used to set Area ID and System ID for the IS-IS.
Up to three NET addresses can 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	Creates IS-IS instances.

Platform Description

N/A

redistribute

Use this command to redistribute routes from one routing protocol into another. 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] }	When redistributing the OSPF routes, filter subtype of the OSPF routes. If the match option is not specified, all routes of the OSPF subtype are received by default. 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*	Sets the metric value for route redistribution, in the range of 0 to 4261412864. If the **metric** option is not specified, the external metric value is used.
metric-type {internal | external}	Sets the metric type of redistributing the route. **internal:** uses the internal metric type. **external:** uses the external metric type. If the metric-type is not specified, **internal** type is used by default.
route-map *map-tag*	Sets the route-map during the external routes redistribution, which is used to filter redistributed routes or set attributions of the routes. The name of *map-tag* must not exceed 32 characters. No route-map is configured by default.
level-1 | level-1-2 | level-2	Specifies the Level of receiving redistributed routing information. If Level is not specified, routing information is redistributed to Level-2 by default. The format is shown as below: **level-1:** redistributes into the Level-1 **level-1-2:** redistributes into both Level-1 and Level-2. **level-2**:redistributes into the Level-2.

Defaults No redistribution is configured by default.

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 in the IP External Reachability Information TLV of LSP when redistributing external route in IPv4 mode.
- The routing information will be placed in the IPv6 Reachable TLV of LSP when redistributing external route in 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 routing calculation. This violates the protocol. In actual application, the priority of the external route may be higher than that of the internal one. 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 one.

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**	Redistributes the reachable routing information from Level-2 into Level-1.
redistribute isis [tag] **level-1 into level-2**	Redistributes the reachable routing information from Level-1 into Level-2.
route-map	Configures the route map.

Platform Description

N/A

redistribute isis level-1 into level-2

Use this command to redistribute Level-1 reachable routing information of the IS-IS instance into 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*	Sets the route map during 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*	Uses the **distribute-list** to filter 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 of *acl-name.*

Defaults Level-1 routes are redistributed into Level-2 in this instance automatically by default.

Command Mode IS-IS routing process configuration mode or IS-IS **address-family ipv6** mode

Usage Guide

- Use the **route-map** or **distribute-list** to filter the Level-1 route of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into Level-1 of current instance.


Caution 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* **level-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	Redistributes routing information from another routing protocol.
redistribute isis *[tag]* level-2 into level-1	Redistributes reachable routing information from Level-2 into Level-1.

Platform Description N/A

redistribute isis level-2 into level-1

Use this command to redistribute Level-2 reachable routing information of the IS-IS instance into Level-2 of current instance. Use the **no** form of this command to disable this redistribution.

redistribute isis [*tag*] **level-2 into level-1** [**route-map** *route-map-name* | **distribute-list** *access-list-name* |*(* **prefix** *ip-address net-mask*| *ipv6-prefix ipv6-address/length)*]

no redistribute isis [*tag*] **level-2 into level-1** [**route-map** *route-map-name* | **distribute-list** *access-list-name* | **(prefix** *ip-address net-mask*| *ipv6-prefix ipv6-address/length)*]

Parameter Description

Parameter	Description
tag	Name of the IS-IS instance
route-map *route-map-name*	Sets the route map during 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*	Uses the **distribute-list** to filter 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 of *acl-name.*
prefix *ip-address net-mask*	Sets routes allowed to be redistributed.
ipv6-prefix ipv6-address/length	Sets ipv6 routes allowed to be redistributed. The routes are specified by the address and the prefix length.

Defaults Disabled

Command mode IS-IS routing process configuration mode or IS-IS **address-family ipv6** mode

Usage Guide Use the **route-map**, **distribute-list** or or **prefix** *ip-address* to filter Level-2 routes of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into Level-1 of current instance.


Caution

You can only choose one of the three parameters **route-map**, **distribute-list** and **prefix** *ip-address*. Routes filtering based on the parameter **prefix** *ip-address* only filters Level-2 routes in your own instance.

Configure the **no distribute isis** [*tag*] **level-2 into level-1** to cancel 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 cancel the instance *tag1* redistribution, while " **no redistritbue isis** *tag1* **level-2 into level-1 route-map** *aa* " will disable **route-map** *aa* filtering during redistribution instead of disabling the instance *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	Redistributes routing information from another routing protocol.
redistribute isis level-1 into level-2	Redistributes reachable routing information from Level-1 into Level-2.

Platform Description N/A

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 No IS-IS instance is configured by default.

Command Mode Global configuration mode

Usage Guide

Use this command to initialize the IS-IS instance and enter 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	Enables the IS-IS IPv4 routing protocol on the interface.
ipv6 router isis	Enables the IS-IS IPv6 routing protocol on the interface.
net	Sets the NET address.

Platform Description N/A

set-overload-bit

Use this command to notify neighbors not to use local IS-IS nodes as a relay to forward data. Use the **no** form of this command to delete the configuration.

set-overload-bit

no set-overload-bit

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command Mode IS-IS routing process configuration mode

Usage Guide

Use this command to force IS-IS node to set overload bit on non-virtual LSP packets. It is used to notify IS-IS neighbors not to use the IS-IS node as a relay to forward data.

Overload bit is used mainly in the following two circumstances:

- When the device is overload

Overload of the local IS-IS nodes such as inadequate memory and full load of CPU will lead to incompleteness of routing table or absence of resource for forwarding data. At this time, you can set overload bit in LSP packet to notify neighbors not to use the local node as a relay. In such a case, overload bit is set or cancelled manually. You must manually delete this command after the local IS-IS node recovers, otherwise the state of overload will persist.

- when you do not want the local IS-IS node to forward real data

If you only want to connect the local IS-IS node to production network for lab use or other functionality use, you can set overload bit in the LSP packets to notify neighbors not to use the local node as a relay for forwarding real data on the network.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# router isis
Ruijie (config-router)# set-overload-bit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

spf-interval

Use this command to set the minimal interval for SPF calculation. Use the **no** form of this command to restore 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 120s.

Defaults This command is not configured by default.
The default SPF interval is 10s, 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 frequent SPF calculation, set and increase the SPF minimal interval. However, increasing the interval also delays the response to the routing change.

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

summary-address

Use this command to configure the IPv4 aggregation route. The **no** form of this command deletes the aggregation route.

summary-address *ip-address net-mask* [**level-1 | level-2 | level-1-2**]

no summary-address *ip-address net-mask*

Parameter Description

Parameter	Description
ip-address	IP address of aggregation route
net-mask	Net mask of aggregation route
level-1	Takes effect on Level-1only.
level-1	Takes effect on Level-2 only.
level-1-2	Takes effect on both Level-1 and Level-2.

Defaults

By default, no aggregation route is configured.
If Level is not specified, it takes effect on Level-2 by default.

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, IS-IS 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	Configures the IPv6 aggregation route.

Platform Description

N/A

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*

Parameter Description

Parameter	Description
ipv6-prefix / prefix-length	Aggregation network address and the IP prefix length of the aggregation network address
level-1	Takes effect on Level-1 only.
level-2	Takes effect on Level-2 only.
level-1-2	Takes effect on both Level-1 and Level-2.

Defaults

By default, no aggregation route is configured.
If Level is not specified, it takes effect on Level-2 by default.

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-addrss	Configures the IPv4 aggregation route.

Platform Description

N/A

show clns is-neighbor

Use this command to show all IS neighbors to provide adjacency relationship information of devices.

show clns [*tag*] **is-neighbors** [*IFNAME* | **detail**]

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance.
IFNAME	Specifies the name of interface.
detail	Shows detailed information.

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The output results of the **show clns is-neighbors detail** command are shown as below:

```
Ruijie# show clns is-neighbors detail
Area (null):
System Id  Type  IP Address  State  Holdtime  Circuit  Interface
r1         L1    1.0.0.2     Up     9         r1.01    GigabitEthernet 0/0
           L2    1.0.0.2     Up     9         r1.01    GigabitEthernet 0/0
  Adjacency ID: 1
  Uptime: 00:00:54
  Area Address(es): 49.1111
SNPA: 00d0.f8bc.de08
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
  Level-1 Protocols Supported: IPv4, IPv6
  Level-2 Protocols Supported: IPv4, IPv6
  BFD(IPv4) session state: Up
  BFD(IPv6) session state: Up
```

Related Commands

Command	Description
show clns neighbors	Shows all IS neighbors to provide the device information and the adjacency relationship of terminal system.

Platform Description N/A

show clns neighbors

Use this command to show all IS neighbors to provide the device information and the adjacency relationship of terminal system.

show clns [*tag*] **neighbors** [*IFNAME* | *detail*]

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance.
IFNAME	Specifies the name of the interface.
detail	Shows detailed information of all interfaces.

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The output results of the s**how clns neighbors detail** command are shown as below:

```
Ruijie# show clns neighbors detail
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	Shows all IS neighbors to provide the device adjacency relationship.

Platform Description N/A

show isis counter

Use this command to show statistics of IS-IS.

show isis [*tag*] **counter**

Parameter Description	Parameter	Description
	tag	IS-IS instance

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The output results of the **show clns neighbors details** command are shown as below:

```
Ruijie# show isis counter
Area (null):
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: 298
isisSysStatLSPErrors: 0
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: 506
isisSysStatLSPErrors: 0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show isis database

Use this command to show the LSP databse information.

show isis [*tag*] **database** [*FLAGS* | *LEVEL* | *LSPID*]

Parameter Description

Parameter	Description
tag	Specifies 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: specifies the LSP database of Level-1. l2 and level-2: specifies the LSP database of Level-2
LSPID	Specifies the ID number of LSP to show the corresponding LSP information only.

Defaults The command has no default setting.

Command Mode Privileged EXEC 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

show isis graceful-restart

Use this command to show the status information related to IS-IS GR.

show isis [*tag*] **graceful-restart**

Parameter Description

Parameter	Description
tag	IS-IS instance name

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

Example 1: The following example shows the GR information of the IS-IS default instance in global configuration mode.

```
Ruijie(config)# show isis graceful-restart
Area (null):
  Graceful-restart Helper: enabled
    Level 1:
      GigabitEthernet 0/0: RR received: 0
    Level 2:
      GigabitEthernet 0/0: RR received: 0
  Graceful-restart: enabled
    Graceful-period: 400s, Level timer: 60s, Interface timer: 3s
    Instance GR status: not restarting
```

Related Commands

Command	Description
graceful-rstart	Enables IS-IS GR Restart.
graceful-rstart grace-period	Configures the maximum interval of grace-restart.
graceful-rstart helper disable	Disable IS-IS GR Help.

Platform Description N/A

show isis hostname

Use this command to show the mapping relation between the hostname of the device and System ID.

show isis [*tag*] **hostname**

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance.

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# show isis hostname
  System ID     Dynamic Hostname     Area (null)
* 5555.5555.5555 Ruijie
  1111.1111.1111 R1

  System ID     Dynamic Hostname     Area 1
* 4444.4444.4444 Ruijie
  2222.2222.2222 R2
```

The example with * refers to the mapping relationship between the hostname of the user's own device and System ID.

The example without * refers to the mapping relationship between the learned hostname (not the hostname of the user's own device) and System ID.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show isis ipv6 topology

Use this command to show the information of IPv6 unicast topology connected with the IS-IS router.

show isis [*tag*] **ipv6 topology** [**l1** | **l2** | **level-1** | **level-2**]

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance
l1	Specifies the Level-1 topology.
level-1	Specifies the Level-1 topology.
l2	Specifies the Level-2 topology
level-2	Specifies the Level-2 topology

Defaults N/A

Command N/A

mode

Usage Guide Privileged EXEC mode

Configuration Examples

```
Ruijie#show isis ipv6 topology
 Area (null):
IS-IS paths to level-1 routers
System Id    Metric   Next-Hop   SNPA            Interface
r1          10      r1        00d0.f822.33ad    GigabitEthernet 0/0
Ruijie       --
IS-IS paths to level-2 routers
System Id    Metric   Next-Hop   SNPA            Interface
r1          10      r1        00d0.f822.33ad    GigabitEthernet 0/0
Ruijie       --
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show isis interface

Use this command to show the detailed information of IS-IS interface.

show isis [*tag*] **interface** [*interface-type interface-number*] [*counter*]

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance name.
interface-type interface-number	Specifies the Interface name.
counter	The number of received and transmitted packets and triggered events

Defaults The command has no default setting.

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):
```

```
GigabitEthernet 0/0  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
Level-1 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s,
Retransmit:5s
Level-1 LSPs in queue: 0
   Number of active level-1 adjacencies: 1
Level-2 Metric: 10/10, Priority: 64, Circuit ID: r1.01
Level-2 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s,
Retransmit:5s
Level-2 LSPs in queue: 0
   Number of active level-2 adjacencies: 1
   Next IS-IS LAN Level-1 Hello in 5 seconds
Next IS-IS LAN Level-2 Hello in 5 seconds
BFD Enabled (Anti-congestion)
```

If (Anti-congestion) is included, BFD enables anti-congestion function. Otherwise the function is not enabled.

```
Ruijie# show isis interface counter
Area (null):
GigabitEthernet 1/1/0:
   IS-IS LAN Level-1 isisCircuitCounterEntry:
     isisCircAdjChanges: 4
     isisCircNumAdj: 2
     isisCircInitFails: 0
     isisCircRejAdjs: 0
     isisCircIDFieldLenMismatches: 0
     isisCircMaxAreaAddrMismatches: 0
     isisCircAuthTypeFails: 0
     isisCircAuthFails: 0
     isisCircLanDesISChanges: 1
   IS-IS LAN Level-2 isisCircuitCounterEntry:
     isisCircAdjChanges: 4
     isisCircNumAdj: 2
     isisCircInitFails: 0
     isisCircRejAdjs: 0
     isisCircIDFieldLenMismatches: 0
     isisCircMaxAreaAddrMismatches: 0
     isisCircAuthTypeFails: 0
```

```
    isisCircAuthFails: 0
    isisCircLanDesISChanges: 1
  IS-IS Level-1 isisPacketCounterEntry:
    isisPacketCountIIHello in/out: 187/278
    isisPacketCountLSP in/out: 10/7
    isisPacketCountCSNP in/out: 0/92
    isisPacketCountPSNP in/out: 0/0
    isisPacketCountUnknown in/out: 0/0
  IS-IS Level-2 isisPacketCounterEntry:
    isisPacketCountIIHello in/out: 186/286
    isisPacketCountLSP in/out: 17/9
    isisPacketCountCSNP in/out: 1/91
    isisPacketCountPSNP in/out: 0/0
    isisPacketCountUnknown in/out: 0/0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show isis mesh-groups

Use this command to show the mesh-group configuraitons on each interface.

show isis [*tag*] **mesh-groups**

Parameter Description	Parameter	Description
	tag	Specifies the IS-IS instance.

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# show isis mesh-groups
Mesh group (blocked)
GigabitEthernet 1/Mesh group 1 :
GigabitEthernet 0/0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

show isis neighbors

Use this command to show the IS-IS neighbor information.

show isis [*tag*] **neighbors** [detail]

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance.
detail	Shows detailed information.

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
ruijie# show isis neighbors detail
 Area (null):
System Id  Type  IP Address    State   Holdtime  Circuit  Interface
r1        L1    1.0.0.2      Up     9        r1.01    GigabitEthernet 0/0
L2    1.0.0.2      Up     9        r1.01    GigabitEthernet 0/0
  Adjacency ID: 1
  Uptime: 00:06:25
  Area Address(es): 49.1111
SNPA: 00d0.f8bc.de08
IPv6 Address(es): fe80::2a9:15ff:fe36:5413
  Level-1 Protocols Supported: IPv4, IPv6
  Level-2 Protocols Supported: IPv4, IPv6
BFD(IPv4) session state: Up
BFD(IPv6) session state: Up
```

When the network type is Broadcast, information in the Circuit column indicates DIS recognized by neighbor r1.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show isis virtual-neighbors

Use this command to display neighbor information in the virtual system of IS-IS.

show isis [*tag*] **virtual-neighbors**

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
uijie# show isis virtual-neighbors
Area (null):
Virtual System Id          Type        State
1111.1111.1111             L1          DOWN
                          L2          UP
2222.2222.2222             L1          DOWN
                          L2          UP
```

UP indicates that the extended LSP fragment is created on a specific level correspondingly.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show isis protocol

Use this command to show information on the IS-IS protocol.

show isis [*tag*] **protocol**

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
IS-IS Router: (null)
  Binding VRF: vrf
  Mib-Binding: off
System ID: 0000.0000.0036   IS-type: level-1-2
  Virtual System ID:
    1111.1111.1111,  2222.2222.2222
  Manual area address(es):
    49.0001,  49.0003
  Interfaces supported by IS-IS:
   GigabitEthernet 0/0,  GigabitEthernet 0/1
  Redistributing IPv4:
isis 1,  isis 2
  Redistributing IPv6:
    isis 3, isis 4
  Distance: 115
  Generate narrow metrics:  Level-1-2
  Accept narrow metrics:    Level-1-2
  Generate wide metrics:    none
  Accept wide metrics:     Level-1-2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show isis topology

Use this command to show the topology of IS-IS node.

show isis [*tag*] **topology** [l1 | l2 | level-1 | level-2]

Parameter Description

Parameter	Description
tag	Specifies the IS-IS instance.
l1	Specifies the topology of Level-1.
level-1	Specifies the topology of Level-1.
l2	Specifies the topology of Level-2.
level-2	Specifies the topology of Level-2..

Defaults The command has no default setting.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie#show isis topology
 Area (null):
IS-IS paths to level-1 routers
System Id    Metric   Next-Hop   SNPA            Interface
r1             10        r1          00d0.f822.33ad      GigabitEthernet
0/0
Ruijie       --
IS-IS paths to level-2 routers
System Id    Metric   Next-Hop   SNPA            Interface
r1          10      r1        00d0.f822.33ad    GigabitEthernet 0/0
Ruijie        --
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

virtual-system

Use this command to set additional system ID for fragments extension in IS-IS routing process configuration mode. Use the **no** form of this command to delete additional system ID.

virtual-system *system-id*

no virtual-system *system-id*

Parameter Description

Parameter	Description
system-id	Additional system ID (6 bytes)

Defaults N/A

Command mode IS-IS routing process configuration mode

Usage Guide This command is used to configure additional system ID of the IS-IS process to generate extended LSP after the 256 fragments of original LSP are filled. To enable fragments extension, the system needs to execute the **lsp-fragment-extend** command after configuring additional system ID

Configuration Examples

```
Ruijie(config)# router isis
Ruijie(config-router)# virtual-system 0000.0000.0034
```

Related Commands

Command	Description
lsp-fragment-extend	Enables fragment extension.

Platform Description N/A

vrf

Use this command to bind the IS-IS instance and VRF in IS-IS routing process configuration mode. Use the **no** form of this command to cancel the binding.

vrf *vrf-name*

no vrf *vrf-name*

Parameter Description

Parameter	Description
vrf-name	The name of the VRF that has been configured.

Defaults N/A

Command mode IS-IS routing process configuration mode

Usage Guide Make sure the VRF has been configured before binding the IS-IS instance and VRF. Before establishing IS-ISv6 adjacency, make sure that VRF is a multi-protocol one and IPv6 is enabled.

Pay attention to restrictions or regulations when configuring IS-IS binding as below:

- The IS-IS instancs within one single non-default VRF must be configured with different system IDs. The IS-IS instancs withindifferent VRFs can be configured with the same system ID.
- An IS-IS instance can be bound with only one VRF while a VRF can be bound with several instances.
- When the VRF bound with the IS-IS instance changes, all IS-IS interfaces related to the instance will be deleted, namely, the ip (ipv6) route isis [tag] configuration on the interfaces will be deleted. Beside, the redistribution configuration in routing process mode will be delete.

Configuration Examples

```
Ruijie(config)#vrf definition vrf_1
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)# router isis
Ruijie(config-router)# vrf vrf_1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Security Commands

ACL Commands

For IDs used in the following commands, refer to the command ID table below.

ID	Meaning
id	Access control list (ACL) ID. Range: Standard IP ACL: in the range from 1 to 99 and from 1300 to 1999 Extended IP ACL: in the range from 100 to 199 and from 2000 to 2699
name	ACL name
sn	ACL SN (products can be set based on priorities)
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, esp, pcp, pim and ip, or it can be numbers 0 to 255 that represent the IP protocol. Important protocols such as ICMP, TCP, and UDP are described separately.
interface idx	Interface index
src	Source IP address of a packet (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 dscp	Differential service code point, and code point value. Range: 0 to 63
flow-label flow-label	Flow label in the range from 0 to 1048575
dst	Destination IP address of a packet (host address or network address)
dst-wildcard	Destination IP address wildcard. It can be discontinuous, for example, 0.255.0.32
fragment	Packet fragment filter Note: Routers do not support packet fragment filter.
precedence precedence	Packet priority (in the range from 0 to 7)
range	Layer 4 port number range of packets

time-range tm-rng-name	Time range of packet filter, named *tm-rng-name*
option	IP packets option. The range is from 0 to 255
log	log option. Outputs matched ACL number and five basic elements information of the packet.
log-input	log-input option. Outputs matched ACL number, name of inbound port and five basic elements of the packet.
user-group	User group.
network-region	Network region
interface	Interface type
tos tos	Types of service of packets (in the range from 0 to 15)
cos cos	CoS values of packets (in the range from 0 to 7)
cos inner *cos*	CoS of packet tags
icmp-type	ICMP message type (in the range from 0 to 255)
icmp-code	ICMP message type code (in the range from 0 to 255)
icmp-message	ICMP message type name
operator port[port]	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, and range-range) *port* indicates the port number. Dyadic operation requires two port numbers, while other operators require only one port number
VID vid	VLAN ID
VID inner vid	VID of the specified inner tag
ethernet-type	Ethernet protocol type. The 0x value can be entered.
match-all tcpf	Match of all bits of the TCP flag
text	Remark text
in	Filter of the incoming packets on an interface
out	Filter of the outgoing packets on an interface
{rule mask offset}$^{+}$	rule: hexadecimal value field; mask: hexadecimal mask field offset: Refer to the offset table. The plus sign (+) indicates at least one group.

The fields in a 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 address	0	O	TTL field	34
B	Source MAC address	6	P	Protocol number	35
C	Data frame length field	12	Q	IP checksum	36

D	VLAN tag field	14	R	Source IP address	38
E	Destination service access point (DSAP) field	18	S	Destination IP address	42
F	Source service access point (SSAP) field	19	T	TCP soure port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version number	26	XY	IP header length and reserved bits	58
K	TOS field	27	Z	Reserved bits and flags bit	59
L	Length of IP packets	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

The offsets of the fields in the preceding table are their offsets in 802.3 data frames of SNAP+tag.

Configuration Related Commands

Global configuration mode command

- **错误!未找到引用源。**
- **错误!未找到引用源。**
- ip access-list logging

The command can configure the smallest print interval of acl logging, and the threshold of matched packets' number of acl loggin print.

IP access-list logging interval *interval*

IP access-list logging threshold *threashold*

Parameter Description	**Parameter**	**Description**
	interval	The smallest print interval of acl logging.
	threshold	The threshold of matched packets' number of acl loggin print.
Defaults	*Interval* is 300， and *threshold* is 1.	
Command Mode	Global Configuration Mode	
Usage Guide	Even a value only matches one of the two conditions（interval or threshold）， the print of acl logging will run. Interval and threshold are not precise parameter, they are just reference values which show when the ACL Logging information should be printed. *Interval* is the interval of printing *acl* logging. The smaller it is, the faster the print frequency will be. Threshold is the matched packets' number. When a number reaches the threshold, the print of acl logging will run.	

Configuration Examples	`Ruijie(config)# ip access-list logging interval 40`
	`Ruijie(config)# ip access-list logging threshold 12000`
	`Ruijie(config)# end`
	Ruijie#	

Related Commands	Command	Description
	show access-lists	**show access-lists**
Platform Description	Only supported by router (software version 10.4(3b13) and above).	

Command History	Version Number	Description
	V10.4	New software version 10.4(3b13)

- ip access-list resequenc
- **错误!未找到引用源。**
- ip access-list logging interval
- ip access-list logging threshold

ACL Configuration Mode Command

- **错误!未找到引用源。**
- **错误!未找到引用源。**
- **错误!未找到引用源。**
- **错误!未找到引用源。**

Interface Mode Command

- **错误!未找到引用源。**
- ipv6 access-list

Use the command to creat IPV6 extended ACL, and access to the mode. Use the “no” command to delete the ACL.

ipv6 access-list *name*

no ipv6 access-list *name*

Parameter Description	**Parameter**	**Description**
	name	ACL name
Defaults	N/A	
Command Mode	Global Configuration Mode	

Configuration Examples	Create IPV6 extended 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 ipv6 access-lists	see ipv6 extended access-lists
Platform Description	N/A	

Command History	Version Number	Description
	V10.0	Software version V10.0 and above.

- ipv6 traffic-filter

access-list

Use this command to create an ACL rule to filter packets.

Use the **no** form of this command to delete the specified ACL entries.

1) Standard IP ACL (in the range from 1 to 99 and from 1300 to 1999)

access-list *id* **{deny | permit} {*source*** *source-wildcard* **| host** *source* **| any | interface** *interface* **| network-region** *region-name* **| user-group** *group-name* **} [time-range** *time-range-name***] [log]**

2) Extended IP ACL (in the range from 100 to 199, from 2000 to 2699, and from 2900 to 3899)

access-list *id* **{deny | permit} protocol {***source source-wildcard* **| host** *source* **| any | interface** *interface* **| network-region** *region-name* **| user-group** *group-name* **} {*destination*** *destination-wildcard* **| host** *destination* **| any | network-region** *region-name* **| user-group** *group-name* **} [precedence** *precedence***] [tos** *tos***] [fragments] [range** *lower upper***] [time-range** *time-range-name***] [option** *option***] [log] [log-input]**

3) List remark

access-list *list-remark text*

Parameter Description

Parameter	Description
id	ACL ID in the range from 1 to 99, from 100 to 199, from 1300 to 1999, from 2000 to 2699, from 2700 to 2899, from 2900 to 2899, and from700 to 799
deny	If matched, access is denied.
permit	If matched, access is permitted.
source	Source IP address of a packet (host address or network address)
source-wildcard	Source IP address 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, or it can be numbers 0 to 255 that represent the IP protocol. Important protocols such as ICMP, TCP, and UDP are described separately.
destination	Destination IP address of a packet (host address or network address)
destination-wildcard	Destination IP address wildcard. It can be discontinuous, for example, 0.255.0.32.
fragment	Packet fragment filter
precedence	Packet priority
precedence	Packet priority value (in the range from 0 to 7)
range	Layer 4 port number range of packets
lower	Lower limit of the Layer 4 port number range of packets
upper	Upper limit of the Layer 4 port number range of packets
time-range	Time range of packet filter
time-range-name	Time range name of packet filter
tos	Types of service of packets

tos	ToS values of packets (in the range from 0 to 15)
icmp-type	ICMP message type (in the range from 0 to 255)
icmp-code	ICMP message type code (in the range from 0 to 255)
icmp-message	ICMP message type name
operator	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, and range-range)
port [*port*]	Port number; *range* requires two port numbers, while other operators require only one port number.
vid *vid*	Match of the specified VID
ethernet-type	Ethernet protocol type
match-all	Match of all the bits of the TCP flag
tcp-flag	TCP flag
log	log option
log-iniput	Log-input option. Enable the matched log information to carry the name of inbound port.
option	The option field of the packet. This field is applied only to the extended ACL named with character string.
option	The option type of packets ()
Interface0-255	Key words of interface type
Interface	Interface type. Such as FastEthernet, Loopback
user-group	User group
group-name	Name of the user group
network-region	Network domain
region-name	Name of the network domain

Defaults No ACL is available by default.

Command Mode Global configuration mode

Usage Guide To filter data by using ACLs, use this command to define a series of ACL rule statements. You can use different types of ACLs based on security requirements.

The standard IP ACL (in the range from 1 to 99 and from1300 to 1999) only controls source IP addresses.

The extended IP ACL (in the range from 100 to 199, from 2000 to 2699, and from 2900 to 3899) controls source and destination IP addresses.

The TCP flag includes part or all of the following:

- urg
- ack
- psh
- rst
- syn
- fin

The packet priority names are as follows:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The types of service are as follows:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The ICMP message types are as follows:

- 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 a port name or 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 a port name or 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 follows:

- aarp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

The options in the IP packet header are as follows:

- add-ext
- any-options
- com-security
- dps
- encode
- eool
- ext-ip
- ext-security
- finn
- imitd
- lsr
- mtup
- mtur
- no-op
- nsapa
- record-route
- router-alert
- sdb
- security
- ssr
- stream-id
- timestamp
- traceroute
- ump
- visa
- zsu

Configuration Examples

Example 1: standard IP ACL

The following basic IP ACL allows packets with the source IP addresses in the range from 192.168.1.64 to 192.168.1.127 to pass.

```
Ruijie(config)# access-list 1 permit 192.168.1.64 0.0.0.63
```

Example 2: extended IP ACL

The following extended IP ACL allows DNS and ICMP messages to pass.

```
Ruijie(config)# access-list 102 permit tcp any any eq domain
Ruijie(config)# access-list 102 permit udp any any eq domain
Ruijie(config)# access-list 102 permit icmp any any echo
Ruijie(config)# access-list 102 permit icmp any any echo-reply
```

Related Commands

Command	Description
show access-lists	Displays all ACLs.

Platform Description

N/A

deny

Use this command to declare one or multiple **deny** conditions used to determine whether to forward or discard packets.

1) Standard IP ACL

[*sn*] **deny** { *source source-wildcard* | **host** *source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } [**time-range** *time-range-name*] [**log**]

2) Extended IP ACL

[*sn*] **deny protocol** {*source source-wildcard* | **host** *source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } {*destination destination-wildcard* | **host** *destination* | **any** | **network-region** *region-name* | **user-group** *group-name* } [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*] [**option** *option*] [**log**] [**log-input**]

Extended IP ACLs of some important protocols:

- **Internet Control Message Protocol (ICMP)**

[*sn*] **deny icmp** {*source source-wildcard* | **host** *source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } {*destination destination-wildcard* | **host** *destination* | **any** | **network-region** *region-name* | **user-group** *group-name* } [*icmp-type* [*icmp-code*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**option** *option*] [**log**] [**log-input**]

- **Transmission Control Protocol (TCP)**

[*sn*] **deny tcp** {*source source-wildcard* | **host** *Source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any** | **network-region** *region-name* | **user-group** *group-name* } [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*] [**option** *option*] [**log**] [**log-input**]

- **User Datagram Protocol (UDP)**

[*sn*] deny udp {*source source –wildcard* | **host** *source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any** | **network-region** *region-name* | **user-group** *group-name* } [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*] [**option** *option*] [**log**] [**log-input**]

3) 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*] [**fragments**] [**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*] [**fragments**]

[**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*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **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*] [**fragments**] [**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 point value, in the range from 0 to 63
flow-label	Flow label
flow-label	Flow label value, in the range from 0 to 1048575
option	Packet option number, in the range from 0 to 255
protocol	For IPv6, the field can be IPV6 | icmp | tcp | udp and number in the range from 0 to 255.

Defaults No entry is available by default.

Command Mode ACL configuration mode

Usage Guide Use this command to configure the filter entries of ACLs in ACL configuration mode

Configuration Examples The following example configures and applies an extended IP ACL on interface 1 to deny the services provided by the source host with the IP address 192.168.4.12 through TCP port 100.

```
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)#
```

The following example configures and applies a standard IP ACL on interface 1 to deny the services provided by the source host with the IP address 192.168.4.12.

```
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
```

The following example configures and applies an extended IPv6 ACL on interface 1 to deny the services provided by the source host with the IP address 192.168.4.12.

```
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 the ACLs.
ipv6 traffic-filter	Applies an extended IPv6 ACL on an interface.
ip access-group	Applies an IP ACL on an interface.
ip access-list	Defines an IP ACL.
ipv6 access-list	Defines an extended IPv6 ACL.
permit	Permits access.

Platform Description N/A

ip access-group

Use this command to apply a specific ACL on an interface in interface configuration mode.

Use the **no** form of this command to cancel the application.

ip access-group { *id* | *name* } { **in** | **out** } [**unreflect**]

no ip access-group { *id* | *name* } { **in** | **out** } [**unreflect**]

Parameter Description

Parameter	Description
id	Specifies the ID of an IP ACL (in the range from 1 to 199, from 1300 to 2699, and from 2900 to 3899).
name	Specifies the name of an IP ACL.

in	Filters the incoming packets on an interface.
out	Filters the outgoing packets on an interface.
unreflect	Disables the Reflexive-ACL.

Defaults No ACL is applied on interfaces by default.

Command Mode Interface configuration mode

Usage Guide Use this command to apply the specified ACL to an interface. Then, the firewall function is enabled.

Configuration Examples The following example applies the ACL 120 on the fastEthernet0/0 to filter 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

ip access-list

Use this command to create a standard or extended IP ACL and enter the corresponding configuration mode.

Use the **no** form of this command to remove the ACL.

ip access-list { **extended** | **standard** } { *id* | *name* }

no ip access-list { **extended** | **standard** } { *id* | *name* }

Parameter Description

Parameter	Description
id	ID of an IP ACL The value ranges from 1 to 99 and from 1300 to 1999 for standard IP ACLs and from 100 to 199, from 2000 to 2699, and from 2900 to 3899 from extended IP ACLs.
name	Name of an ACL

Defaults No ACL is available by default.

Command Mode Global configuration mode

Usage Guide There are differences between a standard ACL and an extended ACL. The extended ACL is more precise. For details, see the **deny** and **permit** commands. Use the **show access-lists command** to

query ACL configuration**.**

Configuration Examples

The following example creates a standard ACL.

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# show ip access-lists
ip access-list standard std-acl
Ruijie(config-std-nacl)#
```

The following example creates an extended ACL.

```
Ruijie(config)# ip access-list extended 123
Ruijie(config-ext-nacl)# show ip access-lists
ip access-list extended 123
```

Related Commands

Command	Description
show ip access-lists	Displays IP ACLs.

Platform Description

N/A

ip access-list logging

Use this command to set the minimum print interval and the match threshold of packets for printing ACL Logging.

IP access-list logging interval *interval*

IP access-list logging threshold *threashold*

Parameter Description

Parameter	Description
interval	The minimum print interval of ACL Logging
Threshold	The match threshold of packets for ACL Logging

Defaults

By default, the interval is 300 and the threshold is 1.

Command mode

Global configuration mode

Usage Guide

Either parameter meeting the requirement triggers the print of ACL Logging.

Neither parameter *interval* nor *threshold* is a precise value. Instead, they are reference values for printing ACL logging.

The *interval* parameter refers to the print interval of ACL logging of the current stream. The smaller the value, the faster ACL logging is printed.

The *threshold* parameter refers to the match count of packets. When the match count reaches the threshold, acl logging will be printed.

Configuration Examples The following example sets the minimum print interval of ACL Logging and the match threshold of packets for ACL Logging

```
Ruijie(config)# ip access-list logging interval 40
Ruijie(config)# ip access-list logging threshold 12000
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show access-lists	Shows the ACL,

Platform Description This command is supported on RGOS 10.4(3b13) or later.

ip access-list resequence

Use this command to rearrange entries of an IP ACL, create an extended IPv6 ACL, and enter the corresponding configuration mode.

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

ip access-list resequence { *id* | *name* } **start-sn inc-sn**

no ip access-list resequence { *id* | *name* }

Parameter Description

Parameter	Description
id	ACL number
name	ACL name
start-sn	Start value of the sequence number
inc-sn	Sequence number increment

Defaults *start-sn*: 10

inc-sn: 10

Command Mode Global configuration mode

Usage Guide Use the **show access-lists** command to view the configuration of this command.

Configuration Examples The following example rearranges the ACL entries.

```
Ruijie# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
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 ACLs.

Platform Description N/A

ipv6 access-list

Use this command to create an extended IPv6 ACL and enter the corresponding configuration mode. Use the **no** form of this command to delete the ACL.

ipv6 access-list *name*

no ipv6 access-list *name*

Parameter Description	Parameter	Description
	name	ACL name

Defaults N/A

Command mode Global configuration mode

Usage Guide Use the **show access-lists** command to view the configuration of this command.

Configuration Examples The following example creates an extended IPv6 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 ipv6 access-lists	Displays extended IPv6 ACLs.

Platform Description N/A

ipv6 traffic-filter

Use this command to apply an IPv6 ACL on the specified interface.

Use the **no** form of this command to remove the application.

ipv6 traffic-filter *name* { **in** | **out** }

no ipv6 traffic-filter *name* { **in** | **out** }

Parameter Description

Parameter	Description
name	Specifies the name of an IPv6 ACL.
in	Filters the incoming packets on an interface.
out	Filters the outgoing packets on an interface.

Defaults No ACL is applied on interfaces by default.

Command Mode Interface configuration mode

Usage Guide Apply the specified IPV6 ACL on an interface to control the interface traffic. You can view the configuration by using the **show ipv6 traffic-filter** command**.**

Configuration Examples The following example applies the **access-list v6-acl** to the gigabit interface Gigabit 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 the ACL configuration on an interface.

Platform Description N/A

list-remark text

Use this command to add remarks for the specified ACL.

Use the **no** form of this command to delete the remarks.

list-remark *text*

Parameter Description

Parameter	Description
Text	Remark information

Defaults N/A

Command Mode ACL configuration mode

Usage Guide Use this command to add remarks for the specified ACL.

Configuration Examples

```
Ruijie# 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 ACLs.
ip access-list	Defines an IP ACL.

Platform Description N/A

no sn

Use this command to delete an ACL entry.

no *sn*

Parameter Description

Parameter	Description
sn	Sequence number of an ACL entry

Defaults N/A

Command Mode ACL configuration mode

Usage Guide Use this command to delete an ACL entry in ACL configuration mode.

Configuration Examples

```
Ruijie(config)# ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)# permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# 12 deny ipv6 host any any
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
12 deny ipv6 any any
Ruijie(config-ipv6-nacl)# no 12
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
10 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)#
```

Related Commands	Command	Description
	show access-lists	Displays all ACLs.
	ip access-list	Defines an IP ACL.
	ipv6 access-list	Defines an extended IPV6 ACL.
	deny	Defines the deny rule for an ACL entry.
	permit	Defines the permit rule for an ACL entry.

Platform Description N/A

permit

Use this command to declare one or multiple **permit** conditions used to determine whether to forward or discard packets.

1) Standard IP ACL

[*sn*] **permit** { *source source-wildcard* | **host** *source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } [**time-range** *time-range-name*] [**log**]

2) Extended IP ACL

[*sn*] **permit protocol** *source source-wildcard* | ***host*** *source* | ***any*** | ***interface*** *interface* | ***network-region*** *region-name* | ***user-group*** *group-name } {destination destination-wildcard* | ***host*** *destination* | ***any*** | ***network-region*** *region-name* | ***user-group*** *group-name } [**precedence** precedence] [**tos** tos] [**fragments**] [**range** lower upper] [**time-range** time-range-name] [**option** option] [**log**] [**log-input**]*

Extended IP ACLs of some important protocols:

- **Internet Control Message Protocol (ICMP)**

[*sn*] **permit icmp** { *source source-wildcard* | **host** *source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } {*destination destination-wildcard* | **host** *destination* | **any** | **network-region** *region-name* | **user-group** *group-name* } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**option** *option*] [**log**] [**log-input**]

- **Transmission Control Protocol** (TCP)

[*sn*] **permit tcp** { *source source-wildcard* | **host** *Source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any** | **network-region** *region-name* | **user-group** *group-name* }[*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*] [**option** *option*] [**log**] [**log-input**]

- **User Datagram Protocol (UDP)**

[*sn*] **permit udp** { *source source –wildcard* | **host** *source* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } [*operator* **port** [*port*]] {*destination destination-wildcard* |**host** *destination* | **any** | **interface** *interface* | **network-region** *region-name* | **user-group** *group-name* } [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*] [**option** *option*] [**log**] [**log-input**]

3) 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*] [**fragments**] [**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*] [**fragments**] [**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*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag*]

- **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*] [**fragments**] [**range** *lower upper*] [**time-range** *time-range-name*]

Parameter Description

Parameter	Description
See the **deny** command.	N/A

Defaults No entry is available by default.

Command Mode ACL configuration mode

Usage Guide Use this command to configure the **permit** conditions for ACLs in ACL configuration mode.

Configuration Examples The following example configures and applies an extended IP ACL on interface 1 to allow the source host with the IP address 192.168.4.12 to provide services through TCP port 100.

```
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)#
```

The following example configures and applies a standard IP ACL on interface 1 to allow the source host with the IP address 192.168.4.12 to provide services.

```
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
```

The following example configures and applies an extended IPv6 ACL on interface 1 to allow the source host with the IP address 192.168.4.12 to provide services.

```
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 ACLs.
ipv6 traffic-filter	Applies an extended IPv6 ACL on an interface.
ip access-group	Applies an IP ACL on an interface.
ip access-list	Defines an IP ACL.
ipv6 access-list	Defines an extended IPv6 ACL.
deny	Denies the access.

Platform Description N/A

remark

Use this command to add remarks to the specified ACE in an ACL.

Use the **no** form of this command to delete the remarks.

remark *text*

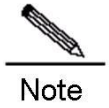
Parameter Description

Parameter	Description
text	Remark information

Defaults N/A

Command mode ACL configuration mode

Usage Guide Use this command to add remarks to the specified ACE.



Note

A remark can contain a maximum of 100 characters. Two same ACE remarks in an ACL are not allowed. When an ACE is deleted, the remark between the ACE and the preceding ACE is also deleted.

Configuration Examples

```
Ruijie# 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 ACLs.
ip access-list	Defines an IP ACL.

Platform Description N/A

show access-group

Use this command to query the ACL configured on an interface.

show access-group [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the ACL configured on the specified interface. If no interface is specified, the ACLs configured on all interfaces will be 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	Defines an IP ACL.
ipv6 traffic-filter	Defines an IPv6 ACL.

Platform Description N/A

show access-lists

Use this command to query all ACLs or the specified ACL.

show access-lists [*id* | *name*]

Parameter Description

Parameter	Description
id	ACL ID
name	ACL name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the specified ACL. If no ID or name is specified, all ACLs will be 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
ipv6 access-list extended v6-acl
```

Related Commands

Command	Description
ip access-list	Defines an IP ACL.
ipv6 access-list	Defines an extended IPv6 ACL.

Platform N/A

Description

show ip access-group

Use this command to query the IP ACL configured on an interface.

show ip access-group [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the IP ACL configured on the specified interface. If no interface is specified, the associated IP ACLs of all interfaces will be 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 ACL.

Platform Description N/A

show ipv6 traffic-filter

Use this command to query the IPv6 ACL configured on an interface.

show ipv6 traffic-filter [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the IPv6 ACL associated with the specified interface. If no interface is specified, the associated IPv6 ACLs of all interfaces will be displayed.

Configuration Examples

```
Ruijie# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 traffic-filter v6 in
Applied On interface GigabitEthernet 0/4.
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 ACL.

Platform Description N/A

Firewall Commands

ip inspect

	Use this command to apply an inspection rule on an interface. Use the **no** form of this command to cancel the application of the inspection rule. **ip inspect** *inspection_name* { **in** | **out** } **no ip inspect** *inspection_name* { **in** | **out** }

Parameter Description

Parameter	Description
inspection_name	Specifies the name of the inspection rule to be applied.
in | **out**	Applies the rule in the inbound or outbound direction of an interface.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide

Use this command to apply an inspection rule on an interface.
When more than one inspection rule is applied in the same direction of an interface, the last one takes effect. Only one inspection rule for multiple special protocols can be applied in one direction of an interface.
Applying an inspection rule for special protocols to an interface (or one direction of an interface) enables the special protocol module of the firewall. The special protocol module of the firewall is automatically disabled when no inspection rule is applied to all interfaces (or all the directions of interfaces).

Configuration Examples

The following example applies the inspection rule abc in the inbound direction of the GigabitEthernet 0/0 interface.

```
Ruijie(config-GigabitEthernet 0/0)#ip inspect spect in
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Note This command is similar to that of Cisco but contains less information

ip inspect name

Use this command to specify an inspection rule for special protocols.

Use the **no** form of this command to remove the rule.

ip inspect name *inspection_name protocol*

no ip inspect name *inspection_name protocol*

Parameter Description

Parameter	Description
inspection_name	Name of an inspection rule
protocol	Protocol to be inspected, including FTP, MMS, RTSP, SIP, H.323, and TCP

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to specify an inspection rule. An inspection rule can apply to multiple special protocols.

Configuration Examples The following example specifies two inspection rules. The rule abc inspects the FTP and MMS protocols and the rule 123 inspects the MMS and H.323 protocols.

```
Ruijie(config)# ip inspect name abc ftp
Ruijie(config)# ip inspect name abc mms
Ruijie(config)# ip inspect name 123 mms
Ruijie(config)# ip inspect name 123 h323
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Note

This command is similar to that of Cisco but contains less information. The alert and audit switches are not available.

show ip inspect

Use this command to query information about an inspection rule for special protocols.

show ip inspect *parameter*

Parameter Description

Parameter	Description
parameter	Displays information about the specified inspection rule. Optional parameters include name *inspection_name*.
interface	Displays information about the inspection rule activated on the interface of a router.
all	Displays information about all inspection rules.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query information about an inspection rule for special protocols.

Configuration Examples

The following example displays information about the inspection rule abc.

```
Ruijie# show ip inspect name abc
Inspection name abc
ftp
mms
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Note This command is similar to that of Cisco but contains less information.

ipmacbind

Use this command to specify an IP-MAC binding rule.

Use the **no** form of this command to delete the rule.

ipmacbind *A.B.C.D H.H.H* [**log**]

no ipmacbind *A.B.C.D H.H.H* [**log**]

Parameter description

Parameter	Description
A.B.C.D	IP address to be bound
H.H.H	MAC address to be bound
log	Whether to enable logging

Defaults The IP-MAC binding function is disabled on the firewall by default.

Command Global configuration mode

Mode

Usage Guide

1. Use this command to specify an IP-MAC binding rule.
2. Configuring a binding rule enables the IP-MAC binding funciton on the firewall.
3. Once all binding rules are deleted, the IP-MAC binding function on the firewall is automatically disabled.
4. A MAC address can be bound with multiple IP addresses. However, an IP address can only be bound with a MAC address.

Configuration Examples

The following example specifies a binding rule.

```
Ruijie(config)# ipmacbind 192.168.52.66 52e1.5d33.aa21 log
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Note Cisco does not have this command.

ipmacbind auto

Use this command to import an IP-MAC binding rule from the ARP table.

ipmacbind auto log

Parameter Description

Parameter	Description
log	Whether to enable logging

Defaults

The IP-MAC binding function is disabled on the firewall by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to import an IP-MAC binding rule from the ARP table. Consequently, the IP-MAC binding function is enabled on the firewall.

Configuration Examples

The following example imports an IP-MAC binding rule from the ARP table.

```
Ruijie(config)# ipmacbind auto
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A


Note Cisco does not have this command.

ipmacbind default action

Use this command to configure the default processing of packets not matching an IP-MAC binding rule. (Permit or deny).

ipmacbind default action { permit | deny }

Parameter Description

Parameter	Description
permit	Permits the packets not matching the IP-MAC binding rule to pass.
deny	Denies the packets not matching the IP-MAC binding rule.

Defaults By default, the packets not matching the IP-MAC binding rule are denied.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example permits the packets not matching an IP-MAC binding rule to pass.

```
Ruijie(config)# ipmacbind default action permit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipmacbind list

Use this command to configure an IP-MAC binding rule list.

ipmacbind list *number*

Parameter Description

Parameter	Description
number	The number of the IP-MAC binding rule list

Defaults By defualt, the IP-MAC binding function of the gateway is disabled.

Command mode Global configuration mode

Usage Guide This command is used to configure an IP-MAC binding rule list.

Configuration Examples The following example configures an IP-MAC binding rule list.

```
Ruijie# configure terminal
Ruijie(config)# ipmacbind list 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipmacbind list number default action

Use this command to apply an IP-MAC binding rule list to the interface and specify the default processing of the packets not matching the IP-MAC binding rule on the curret interface.

ipmacbind list *number* default action { permit | deny [log] }

Parameter Description

Parameter	Description
number	The number of the IP-MAC binding rule list
permit	Permits the packets not matching the IP-MAC binding rule to pass.
deny	Denies the packets not matching the IP-MAC binding rule.

Defaults By defualt, the IP-MAC binding function of the gateway is disabled.

Command mode Interface configuration mode

Usage Guide This command is used to apply an IP-MAC binding rule list to the interface.

Configuration Examples The following example applies an IP-MAC binding rule list to the interface and specifies the default processing of the packets not matching the IP-MAC binding rule on the curret interface.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ipmacbind list 1 default action deny
log
```

Related

Command	Description

Commands		
	N/A	N/A

Platform Description N/A

clear ipmacbind

Use this command to clear an IP-MAC binding rule.

clear ipmacbind { **dynamic** | **all** }

Parameter Description

Parameter	Description
dynamic	Clears all the dynamic IP-MAC binding rules imported from the ARP table.
all	Clears all IP-MAC binding rules.

Defaults The IP-MAC binding function is disabled on the firewall by default.

Command Mode Privileged EXEC mode

Usage Guide Once all IP-MAC binding rules are deleted, the IP-MAC binding function on the firewall is automatically disabled.

Configuration Examples The following example clears all the dynamic IP-MAC binding rules imported from the ARP table.

```
Ruijie# clear ipmacbind dynamic
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Note Cisco does not have this command.

show ipmacbind

Use this command to query information about an IP-MAC binding rule.

show ipmacbind { **table** | **hash** | **statistic** }

Parameter Description

Parameter	Description
table	Displays the IP-MAC binding table.

	hash	Displays the IP-MAC binding hash table.
	statistics	Displays IP-MAC binding statistics (number of lost packets).

Defaults N/A

Command Mode Privilege EXEC mode

Usage Guide Use this command to query information about an IP-MAC binding rule.

The following example displays the global IP-MAC binding rule and the IP-MAC binding rule in the rule list.

```
Ruijie# show ipmacbind table
Totol number of IPMAC-Bind rule: 2
IPMAC-Bind global rule:
No    Type        IP Address      MAC Address     Log
1     <static>    any             00d0.0011.0012  off

IPMAC-Bind list 1 rule:
No     Type        IP Address      MAC Address     Log
1   <static>    192.168.2.2     00d0.0011.0011  off
```

Configuration Examples The following example displays the harsh list of the IP-MAC binding rule.

```
Ruijie(config)# show ipmacbind hash
IPMAC-Bind global:
In MAC hash-list 211:
   1: ip-any, mac-00d0.0011.0012

IPMAC-Bind list 1:
In IP hash-list 616:
1: ip-192.168.2.2, mac-00d0.0011.0011
```

The following example displays statistics on the IP=MAC binding rule.

```
Ruijie(config)# show ipmacbind statistic
IPMAC-Bind global dropped 0 packets
IPMAC-Bind list 1 dropped 0 packets
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Note Cisco does not have this command.

ip ingress-filter

Use this command to enable the filter function on the network ingress.
Use the **no** form of this command to disable the function.

ip ingress-filter [**log**]
no ip ingress-filter [**log**]

Parameter Description

Parameter	Description
log	Whether to enable logging

Defaults The filter function is disabled on the network ingress by default.

Command Mode Interface configuration mode

Usage Guide Use this command to enable the filter function on the network ingress. You can use the no form of this command to disable the function.

Configuration Examples The following example enables the filter function on the network ingress.

```
Ruijie(config)# interface ethernet 1/0
Ruijie(conf-if)# ip ingress-filter log
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A


Note Cisco does not have this command.

show ip ingress-filter

Use this command to query information about the filter function on the network ingress, for example, whether the function is enabled and how many unauthorized flows are blocked.
show ip ingress-filter

Parameter Description

Parameter	Description
N/A	N/A

Defaults The filter function is disabled on the network ingress by default.

Command Mode Priviledge EXECmode

Usage Guide N/A

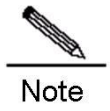
Configuration Examples The following example displays information about the filter function on the network ingress.

```
Ruijie# show ip ingress-filter
Firewall Network-ingress-filter is enable, blocked 0 flows
nterface FastEthernet 1/0: log is on, blocked 0 flows
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A



Note Cisco does not have this command.

ip tcp-intercept list

Use this command to enable the TCP SYN proxy function for the specified network traffic in a direction of an interface.

Use the **no** form of this command to disable the function.

ip tcp-intercept list *extended_ACL_#* { **in** | **out** } [**log**]

no ip tcp-intercept list *extended_ACL_#* { **in** | **out** } [**log**]

Parameter Description

Parameter	Description
extended_ACL_#	Specifies network traffic.
in | out	Enables the funciton in the inbound or outbound direction of an interface.
log	Whether to enable logging.

Defaults The TCP SYN proxy function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to enable the TCP SYN proxy function for the specified network traffic in a direction of an interface. The function must be enabled in interface configuration mode.

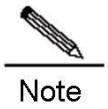
Configuration Examples The following example enables the TCP SYN proxy function for all TCP traffic in the inbound direction of the interface eth 1/0.

```
Ruijie(config)# access-list 100 tcp permit any any
```

```
Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ip tcp-intercept list 100 in log
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A



Note This command is different from that of Cisco. The latter is not related to interfaces and directions.

show ip tcp-intercept

Use this command to query information about the TCP SYN proxy function.

show ip tcp-intercept

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Previledge EXEC mode

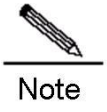
Usage Guide Use this command to query information about the TCP SYN proxy function, including the number of connections denied by the proxy, number of connections permitted by the proxy, and total number of connections.

Configuration Examples The following example displays information about the TCP SYN proxy funciton.

```
Ruijie# show ip tcp-intercept
Intercepting new connections using access-list 100 at Fastethernet 0/1 in
12 incomplete, 5 established connections (total 17)
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A



Note This command is similar to that of Cisco.

ip inspect name tcp

Use this command to configure an insepection rule for TCP (TCP sequence number inspection).
Use the **no** form of this command to remove this rule.

ip inspect name *inspection_name* **tcp**
no ip inspect name *inspection_name* **tcp**

Parameter Description

Parameter	Description
inspection_name	Name of an inspection rule, which is similar to names in ACLs

Defaults N/A

Command Mode Global configuration mode

Usage Guide
Use this command to configure an inspection rule for TCP.
Use the **ip inspect** command to apply the rule to an interface.
Use the **show ip inspect** command to view the rule.

Configuration Examples
The following example configures an inspection rule for TCP named tcp_inspec.

```
Ruijie(config)# ip inspect name tcp_inspec tcp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A


Note

This command is similar to that of Cisco. The alert and audit switches are not available.
This command is related to the **ip inspect name** command. You can use the **ip inspect** command to apply an inspection rule to an interface and the **show ip inspect** command to view the rule.

ip url_filter category

Use this command to set the URL category of a URL filter fule, and add one or more URL categories to a rule.
Use the **no** form of this command to delete a URL category.
ip url_fiter category *url-filter-no url-category*
no ip url_filter category *url-filter-no* [*url-category*]

Parameter

Parameter	Description

Description	*url-filter-no*	URL rule number (ID)
	url-category	URL category

Defaults No URL category is available by default.

Command Mode Global configuration mode

Usage Guide To add a URL category to a URL filter rule, use this command in global configuration mode.
To delete a URL category, use the **no** form of this command.

Configuration Examples The following example adds a URL category named porn to the URL filter rule numbered 10.

```
Ruijie(config)# ip url_filter category 10 porn
```

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

Platform Description N/A

ip url_filter exclusive-domain

Use this command to add or modify a URL filter rule on an interface.
Use the **no** form of this command to delete one or all URL filter rules.
If the current URL request is matched in an URL filter rule, the system will permit or deny the URL; otherwise, the system will take other actions.
ip url_filter exclusive-domain *url-filter-no acl-no action* { **in** | **out** } [**log**]
no ip url_filter exclusive-domain *url-filter-no acl-no action* { **in|out** } [**log**]

Parameter Description	**Parameter**	**Description**
	url-filter-no	URL rule number (ID)
	acl-no	ACL rule number
	action	Action
	block	Deny
	permit	Permit
	{ **in** | **out** }	Applies the rule in the inboud or outbound direction of an interfface.
	in	Inboud direction of an interfface
	out	Outboud direction of an interfface
	log	Enables the logging function for URL filter.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide

To add or modify a URL filter rule, use the url-filter command in global configuration mode. To delete a URL filter rule, use the **no url-filter** command.
Equipment compares packets with filter rules based on the rule creation order. When a rule is matched, the equipment does not check other rules.

Configuration Examples

The following example adds a URL filter rule numbered 10. The ACL number is 100, the action is deny, the default action is permit, the rule is applied in the outbound direction of an interface, and logging is enabled.

```
Ruijie(config-if)# ip url_filter exclusive-domain 10 100 block out log
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip url_filter rule

Use this command to add or modify one or more URLs to a category.
Use the **no** form of this command to remove a URL and its relationship with the corresponding category.
ip url_filter rule *url-category url-addr*
no ip url_filter rule *url-category url-addr*

Parameter Description

Parameter	Description
url-category	URL address category
url-addr	URL address

Command Mode

Global configuration mode

Usage Guide

To filter a URL address, use the URL command in global configuration mode to register the address and its category. To delete a registered URL address, use the **no url** command.
For example, add .sex.com and .sexy.com to the category porn.


Note

The first character of a URL must be a dot (.). In addition, wildcard can only appear at both ends of a rule, instead of in the middle of a string. Registered URL addresses must be level 1 domain names.

Configuration Examples

The following example registers and then deletes a URL address.

```
Ruijie(config)#ip url_filter rule porn .sex.com
Ruijie(config)# no ip url_filter rule porn .sex.com
```

The following example registers and then deletes a URL address prefixed with a wildcard character.

```
Ruijie(config)#ip url_filter rule porn .*sex.com
Ruijie(config)# no ip url_filter rule porn .*sex.com
```

The following example registers and then deletes a URL address sufixed with a wildcard character.

```
Ruijie(config)#ip url_filter rule porn .sex*
Ruijie(config)# no ip url_filter rule porn .sex*
```

The following example registers and then deletes a URL address predixed and sufixed with wildcard characters.

```
Ruijie(config)#ip url_filter rule porn .*sex*
Ruijie(config)# no ip url_filter rule porn .*sex*
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show ip url_filter

Use this command to monitor the URL filter module.

show ip url_filter config { **address|rule|setting** }: displays URL filter configuraiton on routers.

show ip url_filter statistics: displays the inspection statistics of the URL filter module, including the number of packets received from/sent to the content server and number of blocked connections.

Parameter Description	Parameter	Description
	address	URL address conifguration
	rule	URL rule configuration
	setting	URL filter interface application information

Defaults N/A

Command Mode Previledge EXEC mode

Usage Guide The **show ip url_filter config setting** command displays information about the application of URL filter on an interface in interface configuration mode or informaiton about the latest interface entering inteface configuration mode in global configuration mode.

Configuration Examples The following example displays information about URL filter.

sho ip url_filter conf address

```
================[Url without wildcard]===============
cls_name cls-id url-address aaa 1 .tom.com
===========[Url no-wildcard end]====================
================[Relative CLI Command]==============
ip url_filter rule aaa .tom.com
=== [Relative CLI Command To Del the Rules ]==========
```

```
no ip url_filter rule aaa .tom.com
```

show ip url_filter config rule

```
Ip Url_filter Rule configure
Id Attribute Details
-----------------------------------------------
1 contain-class: aaa
================[Relative CLI Command]============
ip url_filter category 1 aaa
====== [Relative CLI Command To Del the Rules ]==========
no ip url_filter category 1 aaa
```

show ip url_filter config setting

```
===== [ Url Filter Rules On gigabitEthernet 0/0 ]========
Rules On Input
Id Acl Action Class-name Url-address
-----------------------------------------------------
1 1 block aaa .tom.com
Relative CLI Command
ip url_filter exclusive-domain 1 1 block in log
Relative CLI Command to Del Rules
no ip url_filter exclusive-domain 1 1 block in log
=====[ Url Filter Rules On gigabitEthernet 0/0 End]=======
```

show ip url_filter statistic

```
show ip url_filter statistics
url filter statistics
the rule 1
Total requests allowed: 0
Total requests blocked: 0
```

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

Platform Description N/A

session-limit

Use this command to limit the number of connections in the specified user range.

session-limit access-group *acl_no* **rate** *rate* **concurrent** *session_no* {**in|out**} [**log**]
no session-limit access-group *acl_no* **rate** *rate* **concurrent** *session_no* **{in|out}** [**log**]

Parameter Description	**Parameter**	**Description**
	acl_no	ACL number corresponding to a rule
	rate	New connection setup rate

session_no	Maximum number of concurrent connections
in | **out**	Connection direction

Defaults The number of connections is not limited by default.

Command Mode Interface configuration mode

Usage Guide Use this command in the outbound direction of an interface.

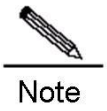
Configuration Examples The following example sets the maximum number of concurrent connections for ACL users to 1000 and allows 100 connections to be created per second.

```
session-limit access-group 1 rate 100 concurrent 10000 in log
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A



Note This command must be executed on the egress interface; otherwise, it does not take effect. This has little impact on the whole efficiency.

ip rate-control

Use this command to enable flow control on each user in the specified user range.

ip rate-control *acl_no* **bandwidth** { **both** | **up|down** } *rate* [**session total** *session_no*] [**rate** *rate_no*]

no ip rate-control *acl_no* **bandwidth** { **both** | **up | down** } *rate* [**session total** *session_no*] [**rate** *rate_no*]

Parameter Description

Parameter	Description
acl-no	ACL number corresponding to a rule
rate	Bandwidth rate (in kbit/s)
session_no	Maximum number of concurrent connections
rate_no	New connection setup rate

Defaults Flow control is disabled by default.

Command Mode Interface configuration mode

Usage Guide The keyword **both** is displayed by default when bandwidth control is configured the same in the

uplink and downlink directions.
This command is executed on the egress interface.

Configuration Examples

The following example sets the maximum bandwidth to 200 kbit/s and the number of concurrent flows to 500 for ACL users, and allows 100 connections to be set up per second.

```
ip rate-control 1 bandwidth both 200 session total 500 rate 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Note

This command must be executed on the egress interface; otherwise, it does not take effect. This has little impact on the whole efficiency.

ip session track-state-strictly

Use this command to enable the strict status track function.
Use the **no** form of this command to disable the function.
Strict status track includes tracking the setup of TCP connecitons and ICMP error messages. The connection will be disconnected when a TCP connection is set up abnormally and the ICMP unreachable message is received.
ip session track-state-strictly
no ip session track-state-strictly

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The strict status track function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

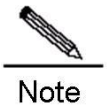
N/A

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A



In some cases, strict status track may cause incorrect reports. Enable the function as required.

ip session filter

Connection filter is used to prevent some unauthorized connection communication. After this command is executed, both the forward and reverse flows are filtered. The filtered packets are discarded and the corresponding flow entry will not be created by the flow platform.

ip session filter *acl_id*

no ip session filter

Parameter Description

Parameter	Description
acl_id	ACL number

Defaults Connection filter is disabled by default.

Command Mode Global configuration mode

Usage Guide

Use this command to configure the connection filter function. The steps are as follows:

1. Defines an ACL.
2. Apply the ACL to connection filter.

This command takes effect globally. After this command is executed, other normal flow communication may be abnormal due to the large specified filter range. Exercise caution when using this command.

Configuration Examples

The following example prevents the communication of dataflows with the source IP address 192.168.1.10.

```
Ruijie(config)#ip access-list standard 1
Ruijie(config-std-nacl)#deny host 192.168.1.10
Ruijie(config-std-nacl)#permit any
Ruijie(config-std-nacl)#exit
Ruijie(config)#ip session filter 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Note This command takes effect globally.

Network Security Protocol (IPSec) Commands

address

Use this command to specify the IP address pool to be issued.

address *low-ip high-ip*

no address *low-ip high-ip*

Parameter Description

Parameter	Description
low-ip	The start IPaddress
high-ip	The end IPaddress

Defaults N/A

Command Mode Address pool configuration mode

Usage Guide Specifiy the IP address pool range for XAUTH clients

Configuration Examples

Example 1: the followin example specified the IP address pool range:

```
Ruijie(config)# crypto isakmp ippool xauth-pool
Ruijie(config-isakmp-ippool)#address 1.1.1.1 1.1.1.200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

authentication (IKE policy)

Use this command to specify the authentication method of the IKE policy in IKE policy configuration mode.

Use the **no** form of this command to restore the default authentication method.

authentication {**pre-share**|**rsa-sig**|digital-email [**asymmetric rsa** | **sm2**] }

no authentication

Parameter Description

Parameter	Description
pre-share	Pre-shared key authentication

rsa-sig	Digital signature authentication
digital-email	Digital envelope certification (*from IPSec VPN Technology Specification*)
rsa	According to the old version *IPSec VPN Technology Specification*, use RSA algorithm digital envelope certification.
sm2	According to the version 2014 *IPSec VPN Technology Specification*, use RSA algorithm digital envelope certification. Double certification is needed.

Defaults

Versions later than RGOS 8.31 use digital signature authentication by default. Versions earlier than RGOS 8.31 use pre-shared key authentication by default.

Command Mode

IKE encryption configuration mode

Usage Guide

Like Cisco, the default authentication method of the current IKE negotiation policy is digital signature authentication. If you want to use pre-shared key authentication, add an IKE policy (configured as pre-shared mode).

Configuration Examples

N/A

Related Commands

Command	Description
crypto isakmp enable	Enables IKE.
encryption { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }	Specifies an encryption algorithm.
hash { **sha** | **md5** | **sm3** }	Specifies the HASH algorithm.
Group	Specifies a Diffie-Hellman group ID.
lifetime	Specifies the lifetime of IKE security association.

Platform Description

N/A

clear crypto isakmp

Use this command to clear a running IKE security association in privileged EXEC mode.

clear crypto isakmp [*connection-id*]

Parameter Description

Parameter	Description
connection-id	ID of an IKE security association

Defaults

If the *connection-id* parameter is not used, this command clears all the existing IKE security

associations.

Command Mode Privileged EXEC mode

Usage Guide Typically, to clear a specific IKE security association, you can first use the **show crypto isakmp sa** command to view the ID of the security association you want to clear, and then use the **clear crypto isakmp** command with the ID to clear the specific IKE security association.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear crypto sa

Use one of the following commands to clear an IPSec security association in privileged EXEC mode.

clear crypto sa

clear crypto sa peer { *ip-address* | *peer-name* }

clear crypto sa map *map-name*

clear crypto sa spi *destination-address* { **ah** | **esp** } *spi*

Parameter Description

Parameter	Description
ip-address	IP address of the remote peer
peer-name	Host name of the remote peer
map-name	Name of crypto map
destination-address	IP address of the local or remote peer
spi	Security parameter index

Defaults If **peer**, **map**, and **spi** are not used to specify an IPSec security list, all IPSec security associations will be cleared.

Command Mode Privileged EXEC mode

Usage Guide

The preceding commands are used to clear IPSec security associations. If such keywords as **peer**, **map**, and **spi** are not used, all IPSec security associations will be deleted by default.

If a security association is established through IKE, it will be cleared. When an interface detects a packet with active IPSec, IPSec will negotiate a new security association. If a security association is established manually, it will be cleared and reestablished immediately.

The newly configured parameters affect only the security associations negotiated subsequently, instead of the existing security associations. To apply the new parameters to the existing security associations, you can clear the existing security associations using this command and negotiate them again.

Clearing a security association will interrupt communication. To prevent communication of other IPSec associations from being interrupted, you must designate a specific security association using **peer**, **map** and **spi**.

If there is only one security association, or no data communication occurs in other security associations, all security associations can be cleared and negotiated again.

Configuration Examples

The following example clears all security associations.

```
Ruijie# clear  crypto  sa
```

Related Commands

Command	Description
clear crypto isakmp	Clears an IKE security association.

Platform Description

N/A

crypto dynamic-map

Use this command to create a dynamic crypto map entry and enter crypto map configuration mode in global configuration mode.

Use the **no** form of this command to remove a crypto map set or an entry.

crypto dynamic-map *dynamic-map-name dynamic-seq-num*

no crypto dynamic-map *dynamic-map-name* [*dynamic-seq-num*]

Parameter Description

Parameter	Description
dynamic-map-name	Specifies the name of a crypto map set.
dynamic-seq-num	Specifies the entry number of the crypto map.

Defaults

No dynamic crypto map is available by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration

N/A

Examples

Related Commands

Command	Description
crypto map(interface IPSec)	Applies the crypto map to an interface.
match address	Specifies an ACL for the crypto map list.
set peer	Specifies a remote peer.
set transform-set	Specifies a transform set.
show crypto map	Displays information about the crypto map.

Platform Description N/A

crypto ipsec df-bit

Use this command to set the DF value of the encapsulation header for all interfaces in global configuration mode.

crypto ipsec df-bit { **clear** | **set** | **copy** }

Parameter Description

Parameter	Description
clear	The external IP header will clear the DF Bit, and routers may split packets and add IPSec encapsulation
set	The external IP header will set DF Bit to 1. However, if the DF Bit of the original IP header is cleared, routers may split packets.
copy	Routers will use the original DF Bit value as the DF Bit value of the external header. **copy** is default.

Defaults This command is disabled by default.

Command Mode Global configuration mode

Usage Guide

Use the **clear** command under IPSec in tunnel mode. You can send packets larger than the MTU value, or you do not know the MTU value.

If this command is enabled without using specific values, routers will use **copy** as the default value.

Configuration Examples The following example clears DF Bit from all interfaces.

```
crypto ipsec df-bit clear
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto ipsec multcast disable

Use this command to disable the IPSec processing of multicast and broadcast packets.

crypto ipsec multcast disable

no crypto ipsec multcast disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

When this command is not executed and ACLs contain multicast and broadcast packets, IPSec processing of the packets is performed.

Command Mode

Global configuration mode

Usage Guide

Use this command to skip IPSec processing if you do not need IPSec processing of multicast packets.

Configuration Examples

This following example disables IPSec processing of multicast and broadcast packets.

```
Ruijie(config)# crypto ipsec multcast disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

crypto ipsec no-filter

Use this command to determine whether to filter decrypted packets.

crypto ipsec no-filter [**list** *acl-number*]

no crypto ipsec no-filter

Parameter Description

Parameter	Description
list *acl-number*	The packet not specified in the ACL is not filtered.

Defaults

Decrypted packets are filtered by default.

Command Mode

Global configuration mode

Usage Guide After this command is configured, dycrpted packets will not be filtered.

Configuration Examples This following example disables dycrypted packet filtering.

```
Ruijie(config)# crypto ipsec no-filter
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto ipsec optional

Use this command to disable IPSec security check in global configuration mode.

crypto ipsec optional

no crypto ipsec optional

Parameter Description

Parameter	Description
N/A	N/A

Defaults This command is disabled by default.

Command Mode Global configuration mode

Usage Guide Data security check will result in significant resource overhead, and disabling this function can save CPU resources. In the model of L2TP over IPSec, L2TP can forcibly enable IPSec, and therefore only IPSec-encrypted packets are allowed. This function can be used as required.

Configuration Examples The following example disables security check.

```
crypto ipsec optional
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto ipsec profile(global IPSec-profile)

Use this command to create or modify the crypto map of a profile in global configuration mode.

Use the **no** form of this command to cancel the crypto map or entry of a profile.

crypto ipsec profile *profile-name*

no crypto ipsec profile *profile-name*

Parameter Description

Parameter	Description
profile-name	Name of the profile with a crypto map set

Defaults

No crypto map is available by default.

Command Mode

Global configuration mode

Use this command to enter crypto map configuration mode of a profile.

Usage Guide

When data is encrypted for protection on a tunnel interface, the crypto map of a profile must be defined and applied to the tunnel interface. The encrypted communication parameters in the profile's crypto map table must be set. The main parameters are as follows:

1. What IPSec security policies will be applied to communication. Those policies are selected from the list consisting of one or more transform sets.
2. Lifetime of security associations
3. Whether security associations are established manually or through IKE
4. For IPv6, IPSec-IPv4, and IPSec-IPv6 tunnels, ACLs must be configured for permit any negotiation. After the crypto map sets of tunnels are applied to tunnel interfaces, all IP traffic passing through the tunnel interfaces is encrypted using the interfaces' crypto map sets. After configuration, IKE negotiation is initiated automatically or when packets from the tunnel interfaces are received. The policy described in the crypto map entry will be used during negotiation of the security association. To carry out IPSec smoothly between two IPSec peers, the tunnel crypto map entries of the two peers must include mutually compatible configuration statements. When two peers try to establish a security association, both of them must have at least one crypto map entry that is compatible with the a crypto map entry of the remote peer and at least meets the following conditions:

1. The crypto map entry must include a compatible encryption ACL (such as mirrored map ACL).
2. The crypto map entries at both sides must identify the address of the peer (unless the peer is using a dynamic crypto map).
3. The crypto map entries must have at least one identical transform set.
4. Only one crypto map set is applied to a single interface. The crypto map set contains IPSec/IKE. Multiple crypto map entries must be created for a single interface if one of the following situations occurs.

1. Different data streams flows on this interface will be processed by different IPSec peers.
2. You want to apply different IPSec securities to different types of traffic (destined to the same or different peers). For example, you want require that the traffic among a group subnets are be authenticated, while the traffic among the other subnets are be authenticated and encrypted. In this case, different types of traffic should be defined in two different ACLs, and an independent crypto map entry must be created for each encryption ACL.

Configuration

The following example configures the crypto map set of a profile (minimum configuration).

Examples

```
Ruijie(config)# crypto ipsec profile profile-name
Ruijie(config-crypto-map)# set transform-set myset
```

Negotiation of IKE security associations

Related Commands

Command	Description
tunnel protection ipsec profile (interface IPSec)	Applies the crypto map to tunnel interfaces.
Set transform-set	Specifies a transform set.
show crypto map	Displays crypto map information.

Platform Description N/A

crypto ipsec rg-sm3

Use this command to enable Ruijie SM3 algorithm. Use the **no** form of this command to restore the default setting.

crypto ipsec rg-sm3
no crypto ipsec rg-sm3

Parameter Description

Parameter	Description
N/A	N/A

Defaults Rujie SM3 algorithm is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to solve SM3 encryption or decryption problems on Ruijie routers.

Configuration Examples The following example enables the Ruijie SM3 algorithm.

```
Ruijie(config)# crypto ipsec rg-sm3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto ipsec security-association idle-time

Use this command to configure automatic disconnection for idle tunnels. Use the **no** form of this command to restore the default setting.

crypto ipsec security-association idle-time *sec*

no crypto ipsec security-association idle-time

Parameter Description

Parameter	Description
sec	Tunnel idle time

Defaults

The tunnel is not torn down automatically by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to tear down the tunnel when the idle time expires. This command takes effect globally.

Configuration Examples

The following example sets the idle time to 120s.

```
Router(config)# crypto ipsec security-association idle-time 120
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

crypto ipsec security-association lifetime

Use this command to modify the global lifetime value used in negotiation of IPSec security associations in global configuration mode.
Use the **no** form of this command to restore the lifetime to the default value.
crypto ipsec security-association lifetime { **seconds** *seconds* | **kilobytes** *kilobytes* }
no crypto ipsec security-association lifetime { **seconds** | **kilobytes** }

Parameter Description

Parameter	Description
seconds *seconds*	Timeout value of a security association (in seconds). The default value is 3600 seconds (1 hour). You can set this parameter to **0**, indicating that the timeout function is disabled.
kilobytes *kilobytes*	Timeout traffic volume of a security association (in kilobytes). The

	default value is 4,608,000 KB. You can set this parameter to **0**, indicating that the byte timeout function is disabled.

Defaults

The default timeout value is 3600 seconds (1 hour) and the default timeout traffic volume is 4,608,000 KB (communication for 1 hour at the rate of 10 Mbit/s).

Command Mode

Global configuration mode

Usage Guide

Traffic encryption of IPSec security associations is based on the shared key. To ensure security, security associations must time out after a specific period of time is due or the specified traffic volume is reached, negotiate again, and use the new shared key. When routers negotiate about security associations, the routers use the smaller one of the lifetime value suggested by the peer and that configured on the local router as the lifetime of the new security association.

There are two types of lifecycles: time lifecycle and traffic volume lifecycle. A security association times out when either of the two lifecycles is due. Change of the global lifecycle only applies to the new security associations negotiated subsequently, instead of existing security associations. To make the new setting take effect as soon as possible, use the **clear crypto sa** command to clear part or all of the contents of the security association database.

To change the global time lifecycle, use the **crypto ipsec security-associationlifetime seconds** command. The time lifecycle specifies that a security association times out after a certain number of seconds elapses. To change the global traffic volume lifecycle, use the **crypto ipsec security-association lifetime kilobytes** command. The traffic volume lifecycle specifies that a security association times out when the traffic volume (in KB) encrypted by using the security association key exceeds a certain quantity.

The shorter the lifecycle value, the more difficult to decrypt the key, because the attacker will use less data to analyze encryption of the same key. However, the shorter the lifecycle, the longer the time that the CPU takes to establish a new security association. Manually established security associations have no lifecycle.

Working principle of lifecycle: A security association (and the related key) times out when either a certain number of seconds (specified by the **seconds** keyword) elapses or a certain number of bytes has occurred in data communication (specified by the **kilobytes** keyword). The new security association starts to negotiate before the original security association reaches its lifecycle limit, to ensure that a new security association is available when the original one times out. The new security association starts to negotiate 30 seconds before the **seconds** lifecycle times out or when the data traffic volume through this tunnel is 256 KB less than the **kilobytes** lifecycle (depending on the one that occurs earlier). If no traffic passs through this tunnel throughout the lifecycle of a security association, negotiation of a new security association will not occur when this security association times out. Accordingly, the new security association begins to negotiate only when IPSec finds a group that should be protected.

The time lifecycle and traffic volume lifecycle can not be set to 0 at the same time; otherwise, negotiation will fail. This configuration will not be checked by system, and must be ensured by users.

Configuration

The following example sets the lifetime of the IPSec security association to 2500 seconds and the

Examples traffic volume lifecycle to 2,304,000 KB (communication for half an hour at the rate of 10 Mbit/s).

```
Ruijie(config)# Crypto ipsec security-association lifetime seconds 2500
Ruijie(config)# Crypto ipsec security-association lifetime kilobytes
2304000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto ipsec security-association replay disable

Use this command to disable the anti-replay function.

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

crypto ipsec security-association replay disable

no crypto ipsec security-association replay disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The replay check function is enabled and is not displayed by default.

Command Mode Global configuration mode

Usage Guide After this command is executed, packet retransmission is not checked, which will improve packet processing efficiency and increase the possibility of being attacked by dos.

Configuration Examples

```
Router(config)# crypto ipsec security-association replay disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto ipsec transform-set

Use this command to define a transform set for the use of a security association.

Use the **no** form of this command to delete a transform set.

crypto ipsec transform-set *transform-set-name transform1*

[*transform2* [*transform3*]]

no crypto ipsec transform-set *transform-set-name*

Parameter Description

Parameter	Description
transform-set-name	Name of a transform set
transform1, transform2, transfrom3	Security protocols and algorithms used by a security association. For details, see the security configuration guide.

Defaults No transform set is available by default.

Command Mode Global configuration mode

Usage Guide

A transform set is a set of security protocols, algorithms, and other settings that will be used in traffic protected by IPSec. During negotiation of IPSec security associations, the peer must use the same transform set to protect the specific data flow.

You can configure multiple transform sets and specify one or more of these transform sets in the crypto map entries. The transform sets defined in the crypto map entries are used to negotiate IPSec security associations to protect the data flows specified by the ACL that corresponds to the crypto map entries. During negotiation, both peers search for the same transform set that exists on both peers. When such a transform set is found, it will be selected and used as a part of the IPSec security association of both peers in the protected traffic.

If a security association is established manually, the same transform set must be specified for the peers at both sides because the manually established association does not negotiate parameters.

Examples

The following example defines a transform set with the protection mode ESP-DES-MD5 (encryption and authentication services are available).

```
Ruijie(config)# crypto ipsec transform-set myset esp-des esp-md5-hmac
```

Related Commands

Command	Description
show crypto ipsec transform-set	Displays information about a transform set.

Platform Description N/A

crypto isakmp authorize

Use this command to enbable domain authentication.

crypto isakmp authorize [*split*]

no crypto isakmp authorize

Parameter Description

Parameter	Description
split	When performing domain authentication, the user name and domain name are split. Only user name

	is required for the authentication

Defaults Domain authentication is disabled.

Command Mode Global configuration mode

Usage Guide Enable domain authentication when the XAUTH is adopted. After the ***splitl*** is specified, the user name and domain name will be split during domain authentication, and only user name is required for the authentication.

Configuration Examples The following example enables domain authentication.

```
Ruijie(config)# crypto isakmp authorize
```

Related Commands

Command	Description
domian	Content of the domain field
crypto isakmp domain-delimiter	Domain delimiter

Platform Description N/A

crypto isakmp client configuration group

Use this command to configure an IKE configuration entry. Use the no form of this command to restore the default setting.

crypto isakmp client configuration group *name*

no crypto isakmp client configuration group *name*

Parameter Description

Parameter	Description
name	IKE configuration entry name

Defaults No IKE configuration entry is created by default.

Command Mode Global configuration mode

Usage Guide After this command is configured and the KEY ID of the client is the same as *name*, corresponding configuration will be pushed to the client.

Configuration Examples The following example configures an IKE configuration entry.

```
Ruijie(config)# crypto isakmp client configuration group cli
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

crypto isakmp domain-delimiter

Use this command to specify the domain delimiter.

crypto isakmp domain-delimiter *keyword* ***[prefix| suffix]***

no crypto isakmp domain-delimiter

Parameter Description	Parameter	Description
	keyword	Domain delimiter
	prefix	Domain delimiter before the indentity authentication character string
	suffix	Domain name locates after the indentity authentication character string

Defaults No domain delimiter is applied.

Command Mode Global configuration mode

Usage Guide The system extract domain name from user identity authentication information according to the domain delimiter.

Configuration Examples The following example specifies a domain delimiter:

```
Ruijie(config)# crypto isakmp domain-delimiter @
```

Related Commands	Command	Description
	crypto isakmp authorize	Enables domain authentication
	domian	Content of the domain field

Platform Description N/A

crypto isakmp enable

Use this command to enbable IKE in global configuration mode. To use IKE for negotiation about the IPSec security association, you must first enable IKE.

Use the **no** form of this command to disable IKE.

crypto isakmp enable

no crypto isakmp enable

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

Defaults IKE is enabled by default.

Command Mode Global configuration mode

Usage Guide Because IKE is enabled by default, there is no need to use this command if you want to use IKE for negotiation about the IPSec security association. If you do not use IKE for negotiation about the IPSec security association, use the **no** form of this command to disable IKE.

Configuration Examples The following example enables IKE.

```
Ruijie(config)# crypto isakmp enable
```

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

Platform Description N/A

crypto isakmp ippool

Use this command to create an address pool to assign IP address for XAUTH clients

crypto isakmp ippool *pool-name*

no crypto isakmp ippool *pool-name*

Parameter Description	**Parameter**	**Description**
	pool-name	Name of address pool

Defaults N/A

Command Mode Global configuration mode

Usage Guide Creating an address pool to assign IP address for XAUTH clients

Configuration Examples The following example enables IKE.

```
Ruijie(config)# crypto isakmp ippool xauth-pool
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

crypto isakmp key

Use this command to specify a pre-shared key to be used in IKE negotiation in global configuration mode.

Use the **no** form of this command to delete the specified pre-shared key.

crypto isakmp key { **0 | 7** } *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] | **ipv6** peer-ipv6-address }

no crypto isakmp key { **0 | 7**} *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] | **ipv6** peer-ipv6-address } [**no-xauth**]

Parameter Description

Parameter	Description
0 | **7**	0 means that plain text is shown for the key, and 7 means that cipher text is shown for the key.
keystring	String of a pre-shared key, which can contain up to 128 characters
peer-hostname	Host name of the remote peer
peer-address	IP address of the remote peer
mask	Address mask when the specified IP address is the address of a network segment
peer-ipv6-address	IPv6 address of the remote peer
no-xauth	Extended authentication is not used.

Defaults No pre-shared key is specified by default.

Command Mode Global configuration mode

Usage Guide IKE typically uses pre-shared negotiation. To allow IKE to successfully establish the IKE security association, you must use this command to configure the same pre-shared key on the two peers that communicate with each other. If the specified peer is a network segment, use the mask to identify its subnet mask. When both peer-address and mask are 0.0.0.0, the default pre-shared key is configured.

Configuration Examples The following example specifies mysecret as the pre-shared key to be used in IKE negotiation with the peer 172.16.1.1.

```
Ruijie(config)# crypto isakmp key 0  mysecret address 172.16.1.1
```

Related	Command	Description

Commands		
	crypto isakmp enable	Enables IKE.
	encryption { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }	Specifies an encryption algorithm.
	hash { **sha** | **md5** | **sm3** }	Specifies the HASH algorithm.
	authentication { **pre-share** | **rsa-sig** }	Specifies an authentication method.
	group { **1** | **2** }	Specifies a Diffie-Hellman group ID.
	lifetime	Specifies the lifetime of the IKE security association.

Platform Description N/A

crypto isakmp keepalive

Use this command to enable a router to send a dead peer detection message to the remote peer in global configuration mode.

For **keepalive** configuration for earlier versions, see the command reference for version 8.2.

crypto isakmp keepalive *secs*

crypto isakmp keepalive *secs* **on-demand**

crypto isakmp keepalive *secs* **periodic**

crypto isakmp keepalive *secs retries*

crypto isakmp keepalive *secs retries* **on-demand**

crypto isakmp keepalive *secs retries* **periodic**

no crypto isakmp keepalive

Parameter Description

Parameter	Description
secs	Tunnel lifetime, in the range from 10 seconds to 3600 seconds
retries	Time interval of packet retransmission, in the range from 2 seconds to 60 seconds

Defaults The dead peer detection message is not sent by default.

Command Mode Global configuration mode

Usage Guide Use this command to allow a router to send the dead peer detection message to the remote peer regularly to check whether the remote peer is alive.

Configuration Examples The following example sets the tunnel idle time to 60 seconds, the time interval of packet retransmission to 5 seconds, and the mode to **on-demand**.

```
crypto isakmp  keepalive  60 5 on-demand
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

crypto isakmp mode-detect

Use the aggressive mode for negotiation when the local security gateway fails to use the main mode to complete the IKE negotiation initiated by the peer end.

crypto isakmp mode-detect

no crypto isakmp mode-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults Only the main mode is used for negotiation if no configuration is performed.

Command Mode Global configuration mode

Usage Guide Now there are many security product vendors who use different ways of implementation. However, there are only two working modes in the first stage of IKE negotiation. To ensure compatibility, the aggressive mode is used automatically by this command for negotiation when the local end fails to complete the IKE negotiation initiated by the peer end.

Configuration Examples The following example automatically recognizes the negotiation initiated in aggressive mode:

```
Ruijie(config)#crypto isakmp mode-detect
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto isakmp nat disable

Use this command to disable the NAT traversal function, which is enabled by default.

crypto isakmp nat disable

no crypto isakmp nat disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The NAT traversal function is enabled by default.

Command Global configuration mode

Mode

Usage Guide Under special conditions, you can use this command to disable the NAT traversal function to communicate with other vendors' device when there are compatibility problems regarding NAT traversal support.

Configuration Examples The following example disables the NAT traversal function.

```
Ruijie(config)# crypto isakmp nat disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto isakmp nat keepalive

Use this command to specify the interval for sending keepalive packets, which can avoid timeout of NAT connections.

crypto isakmp nat keepalive *secs*

no crypto isakmp nat keepalive

Parameter Description

Parameter	Description
secs	Tunnel lifetime, in the range from 5 seconds to 3600 seconds

Defaults The default interval for sending keepalive packets is 5 minutes.

Command Mode Global configuration mode

Usage Guide Use this command to specify the interval for sending keepalive packets. The default interval is 5 minutes.

Configuration Examples The following example sets the interval for sending tunnel keepalive packets to 1 minute.

```
crypto isakmp  nat keepalive  60
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto isakmp next-payload disable

Use this command to configure the next-payload check option.

crypto isakmp next-payload disable

no crypto isakmp next-payload disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, if the unrecognizable doi information appears, negotiation will fail.

Command Mode Global configuration mode

Usage Guide With the next-payload check disabled, the unrecognizable doi field is ignored and negotiation will continue. However, if the reserved field is not 0 or the field length is not matched, negotiation will fail.

Configuration Examples The following example disables the next-payload check.

```
Ruijie(config)# crypto isakmp next-payload disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto isakmp peer

Use this command to select the peer to initiate negotiation first when multiple peers are configured.

crypto isakmp peer { **bind** | **random** }

no crypto isakmp policy

Parameter Description

Parameter	Description
bind	Takes effect only in 3G environments. 3G cards are configured with multi-peer dialing, which is bound with the peer address of IPSec dialing. The first dialing configuration group corresponds to the first peer configuration based on the configuration order.
random	Selects the peer that initiates negotiation first randomly.

Defaults By default, the first peer attempts to initiate negotiation based on the configuration order.

Command Mode Global configuration mode

Usage Guide When used with 3G links, 3G dialing is configured with multiple dialing address groups, which have a one-to-one relationship with the peer configuration in the IPSec map. The peer binding function can be enabled to speed up dialing.
If the preceding configuration is unavailable, the corresponding peer can be found after multiple retries, and it takes a long time to establish tunnel for the first time.

Configuration Examples The following example enables the function of randomly selecting the tunnel connection address.

```
Ruijie(config)# crypto isakmp peer random
```

Related Commands

Command	Function
set peer	Specifies a remote peer in the crypto map entry.

Platform Description N/A

crypto isakmp policy

Use this command to define a policy with a certain priority for IKE and enter IKE policy configuration mode in global configuration mode.
Use the **no** form of this command to delete a policy with a certain priority.
crypto isakmp policy *priority*

no crypto isakmp policy *priority*

Parameter Description

Parameter	Description
priority	Priority of an IKE policy, an integer in the range from 1 to 10000, where 1 represents the highest priority and10000 represents the lowest priority.

Defaults No default priority is available by default.

Command Mode Global configuration mode

Usage Guide Use this command to specify the parameters for IKE negotiation about the IKE security association. Run this command to enter IKE policy configuration mode. In IKE policy configuration mode, set the following parameters:
encryption(IKE policy): default value = 56-bit DES-CBC
hash(IKE policy): default value = SHA-1
authentication(IKE policy): default value = RSA signature

group(IKE policy): default value = 768 bits
Diffie-Hellmanl lifetime(IKE policy): default value = 86400 seconds (1 day)
If the value of a parameter is not specified, the default value of this parameter will be used. Multiple IKE policies can be configured on a router. Before IKE negotiation begins, the router tries to find the public policies configured at both sides, starting from the policy with the highest priority specified on the remote peer.

Configuration Examples

The following example configures an IKE policy with the priority 100.

```
Ruijie(config)# crypto isakmp policy 100
Ruijie(isakmp-policy)# authentication pre-share
Ruijie(isakmp-policy)# encryption des
Ruijie(isakmp-policy)# group  2
Ruijie(isakmp-policy)# hash  sha
Ruijie(isakmp-policy)# ^Z
Ruijie# show crypto isakmp policy
Protection suite of priority 100
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Secure Hash Standard
authentication method:  Pre-Shared Key
Diffie-Hellman group:  #2 (1024 bit)
lifetime:             3600 seconds
Default protection suite
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Secure Hash Standard
authentication method:  Rsa-Sig
Diffie-Hellman group:  #1 (768 bit)
lifetime:             3600 seconds
```

Related Commands

Command	Description
crypto isakmp enable	Enables IKE.
encryption { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }	Specifies an encryption algorithm.
hash { **sha** | **md5** | **sm3** }	Specifies the HASH algorithm.
authentication { **pre-share** | **rsa-sig** }	Specifies an authentication method.
group	Specifies a Diffie-Hellman group ID.
lifetime	Specifies the lifetime of IKE security association.

Platform Description

N/A

crypto isakmp rg-sm1

Use this command to enable Ruijie IKE negotiation mode for IKE encryption algorithm.

crypto isakmp rg-sm1
no crypto isakmp rg-sm1

Parameter Description

Parameter	Description
N/A	N/A

Defaults Ruijie IKE negotiation mode is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to solve encryption or decryption problems during SM1 negotiation on Ruijie routers.

Configuration Example The following example enables Ruijie IKE negotiation mode.

```
Ruijie(config)# crypto isakmp rg-sm1
```

Related Commands

Command	Function
N/A	N/A

Platform Description N/A

crypto isakmp session limit

Use this command to set a limit on the number of IKE sessions. Use the no form of this command to restore the default setting.

crypto isakmp session limit *number*
no crypto isakmp session limit

Parameter Description

Parameter	Description
number	Sets a limit on the number of IKE sessions, in the range from 5 to 1024.

Defaults No limit is set on the IKE session number by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example The following example sets a limit on the number of IKE sessions.

```
Ruijie(config)# crypto isakmp session limit 5
```

Related Commands

Command	Function
N/A	N/A

Platform Description N/A

crypto isakmp vendorid disable

Use this command to disable the sending of Ruijie vendor information during IKE negotiation.

crypto isakmp vendorid disable

no crypto isakmp vendorid disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults IKE negotiation carries Ruijie vendor information by default.

Command Mode Global configuration mode

Usage Guide The private VIDs of some vendors are unrecognizable during IKE negotiation, causing negotiation failure. Use this command to disable the sending of Ruijie's VID information.

Configuration Example The following example disables the sending of VID information.

```
Ruijie(config)# crypto isakmp vendorid disable
```

Related Commands

Command	Function
N/A	N/A

Platform Description N/A

crypto isakmp xauth cisco_comp

Use this command to adopt cisco's compatible extended authentication for IKE negotiation. Use the **no** form of this coammnd to restore the default setting.

crypto isakmp xauthcisco_comp

no crypto isakmp xauth cisco_comp

Parameter Description

Parameter	Description
N/A	N/A

Defaults This command is not configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example The following example adopts cisco's compatible extended authentication for IKE negotiation.

```
Ruijie(config)# crypto isakmp xauth cisco_comp
```

Related Commands

Command	Function
N/A	N/A

Platform Description N/A

crypto isakmp xauth timeout

Use this command to configure the identity authentication timeout period of extended authentication.

crypto isakmp xauth timeout*secs*

no crypto isakmp xauth timeout

Parameter Description

Parameter	Description
secs	Timeout period of extended authentication, in the range from 5 seconds to 90 seconds.

Defaults The default timeout period of extended authentication is 15 seconds.

Command Mode Global configuration mode

Usage Guide Use this command to configure the timeout period of extended authentication. You can set the timeout period to a large value when network delay occurs or the authentication server is slow.

Configuration Example The following example configures the timeout period of extended authentication.

```
Ruijie(config)# crypto isakmp xauth timeout 30
```

Related Commands

Command	Function
N/A	N/A

Platform Description N/A

crypto isakmp link-redundency

Configure TRACK and DLPD protocol monitored by IPSEC in a multiple linkage scenario.

crypto isakmp link-redundency backup *backup_interface* **track** *track_id*

no crypto isakmp link-redundency backup *backup_interface* **track** *track_id*

crypto isakmp link-redundency backup *backup_interface* **dldp** *master_interface*

no crypto isakmp link-redundency backup *backup_interface* **dldp** *master_interface*

Parameter Description

Parameter	Description
backup_interface	When the TRACK and DLDP protocol is up, the IPSEC tunnel in the backup link will be deleted.
track_id	The *track_id* monitored by IPSEC.
master_interface	IPSEC monitors interface configured with DLPD.

Defaults By default, IPSEC does not monitor any TRACK and DLPD protocol.

Command Mode Global configuration mode

Usage Guide In a scenario where there is a primary linkage, backup linkage or multiple linkage, the IPSec is used to monitor the status of primary linkage. When

the primary linkage is up, the IPSec channel in the backup linkage will be removed so as to clear the reverse routing. And then the normal data forwarding is guranteed.Currently, TRACK and DLDP are used to monitor primary linkage.

Configuration Example

The following example configures the timeout period of extended authentication.

```
Ruijie(config)# crypto isakmp link-redundency backup Async 1 track 1
Ruijie(config)# crypto isakmp link-redundency backup Async 1 dldp
GigabitEthernet 0/0
```

Related Commands

Command	Function
ip rns *rns_id* **track** *track_id* **rns** *rns_id*	Configures the TRACK on the primary linkage.
dldp *peeer_addr*	Configures the DLDP on the primary linkage.

Platform Description

N/A

Command History

Version Number	Description
10.4(3b13)	new

crypto map (global IPSec)

Run this command to create or modify a crypto map in global configuration mode.

Use the **no** form of this command to remove a crypto map or an entry.

crypto map *map-name seq-num* **ipsec-manual**

crypto map *map-name seq-num* **ipsec-isakmp** [**dynamic** *dynamic-map-name*]

no crypto map *map-name* [*seq-num*]

Parameter Description

Parameter	Description
map-name	Name of the crypto map set
seq-num	Sequence number of the crypto map entry
ipsec-manual	Specifies a map entry for manually establishing the IPSec security association.
ipsec-isakmp	Specifies a map entry for establishing the IPSec security association negotiated through IKE.
dynamic-map-name	Specifies the name of the dynamic crypto map set used as the policy template.

Defaults

No crypto map is avaiable by default.

Command Mode

Global configuration mode. You will enter crypto map configuration mode when using this command.

Usage Guide

To use IPSec for data encryption, you must first define a crypto map and apply the crypto map to the specific interfaces. Define the traffic encryption parameters in the crypto map, including:

- What traffic should be protected by IPSec: Associate the configured encryption ACL.
- Where the traffic protected by IPSec will be sent to: Which is the remote IPSec peer.
- Local address used for IPSec communication: Apply the crypto map set to the interface. IPSec uses the address of the communication interface as the address of the local peer.
- Which IPSec security policies should be applied to the traffic: Choose from the list that consists of one or more transform sets.
- Lifetime of the security association
- Whether the security association is established manually or through IKE.

The crypto map entries that have the same crypto map name (but with different map sequence numbers) constitute a crypto map set. Apply the crypto map set to the interface so that all the IP traffic that passes this interface is determined based on the crypto map set applied to the interface. If a crypto map entry finds an outbound IP channel that should be protected and the crypto map specifies the use of IKE, the security association will be negotiated with the remote peer based on the parameters in this crypto map entry. If the crypto map entry specifies use of the manually established security association, then a security association must have been established during configuration. The data is encrypted for transmission once the security association is established successfully either manually or through IKE negotiation. If negotiation of the security association fails, the data is discarded.

The policy described in the crypto map entry will be used during negotiation of the security association. To carry out IPSec smoothly between two IPSec peers, the crypto map entries of the two peers must include mutually compatible configuration statements. When two peers try to establish a security association, both of them must have at least one crypto map entry that is compatible with the a crypto map entry of the remote peer and at least meets the following conditions:

- The crypto map entry must include a compatible encryption ACL (such as mirrored map ACL).
- The crypto map entries at both sides must identify the address of the peer (unless the peer is using a dynamic crypto map).
- The crypto map entries must have at least one identical transform set.
- Only one crypto map set is applied to a single interface. The crypto map set contains IPSec/IKE or combination of IPSec/manual entry. If you create multiple crypto map entries for a given interface, you need to use the *seq- num* parameter of the map entry to sort these map entries again. The smaller the *seq-num* value, the higher the priority.

Multiple crypto map entries must be created for a single interface if one of the following situations occurs.

- Different data flows on this interface will be processed by different IPSec peers.
- You want to apply different IPSec securities to different types of traffic (destined to the same or different peers). For example, you require that the traffic among a group subnets be authenticated, while the traffic among the other subnets be authenticated and

encrypted. In this case, different types of traffic should be defined in two different ACLs, and an independent crypto map entry must be created for each encryption ACL.

For the use of a dynamic crypto map, see the usage guide of the **crypto dynamic-map** command.

Configuration Examples

The following two examples show the minimum configuration of a manual IPSec security association and an IKE-negotiated IPSec security association.

Manual IPSec security association

```
Ruijie(config)# crypto map mymap 3 ipsec-manual
Ruijie(config-crypto-map)# set peer 2.2.2.2
Ruijie(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
Ruijie(config-crypto-map)# set sesession-key outbound esp 300 cipher abcdef1234567890
Ruijie(config-crypto-map)# set transform-set myset
Ruijie(config-crypto-map)# match address 101
```

IKE-negotiated security association

```
Ruijie(config)# crypto map mymap 4 ipsec-isakmp
Ruijie(config-crypto-map)# set peer 2.2.2.2
Ruijie(config-crypto-map)# set transform-set myset
Ruijie(config-crypto-map)# match address 101
```

Related Commands

Command	Description
crypto map(interface IPSec)	Applies the crypto map to an interface.
match address	Specifies an ACL for the crypto map list.
Set peer	Specifies a remote peer.
Set transform-set	Specifies a transform set.
show crypto map	Displays information about the crypto map.

Platform Description

N/A

crypto map (interface IPSec)

Use this command to apply the predefined crypto map set to an interface in interface configuration mode.

Use the **no** form of this command to cancel the association of the crypto map set on an interface.

crypto map *map-name*

no crypto map [*map-name*]

Parameter Description

Parameter	Description
map-name	Name of the crypto map

Defaults No crypto map is applied to an interface by default.

Command Mode Interface configuration mode

Usage Guide Use this command to apply the crypto map set to an interface. To provide IPSec encryption protection for the data on this interface, you must apply a crypto map set to this interface. Only one crypto map set can be associated with a single interface. If multiple crypto map entries have the same *map-name* but different *seq-num*, they are in the same set and applied to the same interface. The crypto map entry with a smaller s*eq-num* has a higher priority and is determined first.
One crypto map set can be applied only on one interface.

Configuration Examples The following example applies the crypto map named **mymap** to the interface s0.

```
Ruijie(config)# interface  serial  0
Ruijie(config-if)# crypto map mymap
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.

Platform Description N/A

crypto map client accounting

Use this command to configure AAA for the Radius accounting. Use the **no** form of this command to restore the default setting.

crypto map *map-name* **client accounting list** *aaa-name*

no crypto map *map-name* **client accounting list**

Parameter Description

Parameter	Description
map-name	Name of the crypto map
aaa-name	AAA accounting name

Defaults No AAA is configured by default

Command Mode Global configuration mode

Usage Guide Use this command to implement Radius accounting by using AAA.
IPSec extended authentication and accounting is mandatory for SMP Radius authentication.

Configuration Examples

The following example configures AAA for the Radius accounting.

```
Router(config)#aaa new-model
Router(config)#aaa accounting update periodic 1
Router(config)#aaa accounting update
Router(config)#aaa accounting network default start-stop group radius
Router(config)#aaa authentication xauth vpn group radius
Router(config)#crypto map mymap client authentication list vpn
Router(config)#crypto map mymap client accounting list default
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

crypto map client authentication

Use this command to configure AAA for the Radius authentication. Use the **no** form of this command to restore the default setting.

crypto map *map-name* **client authentication list** *aaa-name*

no crypto map *map-name* **client authentication list**

Parameter Description

Parameter	Description
map-name	Name of the crypto map
aaa-name	AAA authentcation name

Defaults

No AAA is configured by default

Command Mode

Global configuration mode

Usage Guide

Use this command to implement Radius authentication by using AAA.
IPSec extended authentication should be used with AAA xauth mode.

Configuration Examples

The following example configures AAA for the Radius authentication.

```
Router(config)#aaa new-model
Router(config)#aaa accounting update periodic 1
Router(config)#aaa accounting update
Router(config)#aaa accounting network default start-stop group radius
Router(config)#aaa authentication xauth vpn group radius
Router(config)#crypto map mymap client authentication list vpn
Router(config)#crypto map mymap client accounting list default
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

crypto map local-address

Use this command to specify the fixed local address of IPSec in global configuration mode.
Use the **no** form of this command to remove the designated local address of IPSec.
crypto map *map-name* **local-address** *interface-type interface-number*
no crypto map *map-name* **local-address**

Parameter Description	Parameter	Description
	map-name	Name of the IPSec crypto map
	interface-type interface-number	Interface type and number used as the local address of IPSec

Defaults The address of the interface through which IPSec data goes out is used as the local address of IPSec.

Command Mode Global configuration mode

Usage Guide
If one crypto map is applied to multiple interfaces and this command is not used, RGOS will create an IPSec security association on each interface for the same remote peer and the same traffic. By default, the IP address of the interface through which the encrypted traffic goes in and out is used as the local address. After a local address is specified using this command, applying the same crypto map to several interfaces creates only one IPSec security association, which will be used for communication.
If a router has multiple interfaces that allow IPSec communication, this command can be used to specify the local address of IPSec to facilitate management. In this way, RGOS uses a single fixed address to communicate with external routers.
Generally, it is recommended that the loopback address be used as the local address of IPSec.

Configuration Examples
The following example specifies the Loopback0 address as the local address of IPSec.

```
interface serial0
crypto map mymap
interface serial1
crypto map mymap
crypto map mymap local-address loopback0
```

Related Commands	Command	Description
	crypto isakmp enable	Enables IKE.
	encryption	Specifies an encryption algorithm.

hash { **sha** | **md5** | **sm3** }	Specifies the HASH algorithm.
authentication { **pre-share** | **rsa-sig** }	Specifies an authentication method.
group	Specifies a Diffie-Hellman group ID.
lifetime	Specifies the lifetime of the IKE security association.

Platform Description N/A

crypto mib enable

Use this command to enable the IPSec MIB function before you access the MIB node of IPSec.

Parameter Description

Parameter	Description
N/A	N/A

Defaults The IPSec MIB statistical function is disabled by default.

Command Mode Global configuration mode

Usage Guide IPSec MIB management involves collecting statistics on data flows and encrypted/decrypted packets and it may affect the performance of IPSec data communication. Therefore, the IPSec MIB statistical function is disabled by default. To access the MIB node of IPSec, enable the IPSec MIB function by using the CLI command.

Configuration Examples

The following example enables the IPSec MIB function.

```
crypto mib enable
```

The following example disables the IPSec MIB function.

```
no crypto mib enable
```

Related Commands

Command	Description
Ruijie(config)# crypto mib enable	Enables the IPSec MIB statistcial function.

crypto software

Use this command to continue using software encryption after a hardware encryption card is configured on a router.

Parameter Description

Parameter	Description
N/A	N/A

Defaults Hardware encryption is used automatically after a hardware encryption module is inserted into a router.

Command Mode Global configuration mode

Usage Guide If no encryption card is inserted, software encryption is used automatically without the need of using this command. If an encryption card is inserted and this command is executed, software encryption is used. If an encryption card is inserted and this command is not executed, hardware encryption is used.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug crypto engine

Use this command to query debug messages related to IPSec processing.

debug crypto engine

no debug crypto engine

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privilege EXEC mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug crypto ipsec

Use this command to query debug messages related to IPSec processing.

debug crypto ipsec

no debug crypto ipsec

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

debug crypto isakmp

Use this command to query debug messages related to IKE events.

debug crypto isakmp

no debug crypto isakmp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Example N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug crypto pool

Use this command to show the debug message related to the IKE pool.

debug cryptopool

no debug crypto pool

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

dns

Use this command to configure a DNS server address and push the address to the client. Use the **no** form of this command to restore the default setting.

dns *pri-ip-addres* [*second-ip-address*]

no dns

Parameter Description

Parameter	Description
pri-ip-addres	Specifies a primary DNS server address.
second-ip-address	Specifies a secondary DNS server address.

Defaults No DNS server address is configured by default.

Command Mode config-isakmp-group mode

Usage Guide The DNS server address will be pushed to the client.

Configuration Examples The following example specifies a DNS server address.

```
Router(config-isakmp-group)#dns 1.1.1.1 1.1.1.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

domain

Use this command to specify a domain name and associates the domain with a VRF. Use the **no** form of this command to restore the default setting.

domain *domain-name* **[vrf]** [*vrf-name*]
no domain *domain-name*

Parameter Description

Parameter	Description
domain-name	Specifies a domain name.
vrf-name	Specifies a VRF name.

Defaults No domain name is configured by default.

Command config-isakmp-group mode

Mode

Usage Guide During XAUTH authentication, if the domain name contained by the packet is the same as the specified domain name, the username will be separated. If a VRF is configured, the matching domain name will be allocated to the VRF.

Configuration Examples The following example specifies a domain name and associates the domain with VRF VPNA.

```
Router(config-isakmp-group)#domain ruijie vrf VPNA
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

encryption (IKE policy)

Use this command to specify the encryption algorithm of the IKE policy in IKE policy configuration mode.
Use the **no** form of this command to restore the default value.
encryption {**des**|**3des|aes-128|aes-192|aes-256**}

no encryption

Parameter Description

Parameter	Description
des	Specifies the 56-bit DES-CBC as the encryption algorithm.
3des	Specifies the 168-bit 3DES-CBC as the encryption algorithm.
aes-128	Specifies the AES of the 128-bit key length as the encryption algorithm.
aes-192	Specifies the AES of the 192-bit key length as the encryption algorithm.
aes-256	Specifies the AES of the 256-bit key length as the encryption algorithm.

Defaults The 56-bit DES-CBC encryption algorithm is the default encryption algorithm.

Command Mode IKE policy configuration mode

Usage Guide Different from the encryption algorithm of the IPSec security association, the data encryption algorithm specified by this command is used to encrypt the data of the IKE security association.

Configuration Examples The following example specifies the encryption algorithm of the IKE policy as DES.

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# encryption des
```

Related

Command	Description

Commands

crypto isakmp enable	Enables IKE.
hash { **sha** | **md5** | **sm3** }	Specifies the HASH algorithm.
authentication { **pre-share** | **rsa-sig** }	Specifies an authentication method.
group { **1** | **2** }	Specifies a Diffie-Hellman group ID.
lifetime	Specifies the lifetime of the IKE security association.

Platform Description

N/A

group (IKE policy)

Use this comand to specify the Diffie-Hellman group ID in the IKE policy in IKE policy configuration mode.

Use the **no** form of this command to restore the Diffie-Hellman group ID to the default value.

group { **1|2** }

no group

Parameter Description

Parameter	Description
1	Specifies the 768-bit Diffie-Hellman group.
2	Specifies the 1024-bit Diffie-Hellman group.
5	Specifies the 1536-bit Diffie-Hellman group.

Defaults

The 768-bit Diffie-Hellman group (group 1) is the default Diffie-Hellman group ID in the IKE policy.

Command Mode

IKE policy configuration mode

Usage Guide

Use this command to specify the Diffie-Hellman group used in the IKE policy.

Configuration Examples

The following example specifies the Diffie-Hellman group in the IKE policy as 1024 bits.

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# group 2
```

Related Commands

Command	Description
crypto isakmp enable	Enables IKE.
encryption { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }	Specifies an encryption algorithm.
hash { **sha** | **md5** }	Specifies the HASH algorithm.
authentication { **pre-share** | **rsa-sig** }	Specifies an authentication method.
lifetime	Specifies the lifetime of the IKE security association.

Platform Description	N/A

hash (IKE policy)

Use this command to specify the HASH algorithm in the IKE policy in IKE policy configuration mode.
Use the **no** form of this command to restore the hash algorithm to the default value.
hash { **sha** | **md5** | **sm3** }
no hash

Parameter Description

Parameter	Description
sha	Specifies SHA-1 (HMAC variant) as the HASH algorithm.
md5	Specifies MD5 (HMAC variant) as the HASH algorithm.
sm3	Specifies SM3 (HMAC variant) as the HASH algorithm.

Defaults The default HASH algorithm is SHA.

Command Mode IKE policy configuration mode

Usage Guide Use this command to specify the HASH algorithm used in the IKE policy.

Configuration Examples The following example sets the HASH algorithm to md5.

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# hash md5
```

Related Commands

Command	Description
crypto isakmp enable	Enables IKE.
encryption { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }	Specifies an encryption algorithm.
authentication { **pre-share** | **rsa-sig** }	Specifies an authentication method.
group	Specifies a Diffie-Hellman group ID.
lifetime	Specifies the lifetime of the IKE security association.

Platform Description	N/A

key

Use this command to configure the pre-shared key. Use the **no** form of this command to restore the default setting.

key { **0** | **7** } *keystring*

no key

Parameter Description	**Parameter**	**Description**
	**0	7**	0 indicates plain text and 7 indicates encrypted text.
	keystring	Configures the key string (128 characters max).

Defaults No pre-shared key is configured by default.

Command Mode config-isakmp-group mode

Usage Guide This command is valid only in active mode during KEY ID authentication.

Configuration Examples The following example configures the pre-shared key.

```
Router(config-isakmp-group)# key 0  mysecret
```

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

Platform Description N/A

lifetime (IKE policy)

Use this command to specify the lifetime of the IKE security association in IKE policy configuration mode.

Use the **no** form of this command to restore the lifetime to the default value.

lifetime *seconds*

no lifetime

Parameter Description	**Parameter**	**Description**
	seconds	IKE lifetime value (in seconds), which is an integer in the range from 60 seconds to 86,400 seconds

Defaults 86,400 seconds (1 day)

Command Mode IKE policy configuration mode

Usage Guide Use this command to specify the lifetime of the IKE security association. When IKE starts negotiation, it first ensures consistency of security parameters for its sessions. Then, these parameters are referenced by the IKE security association on each peer and retained on each

peer until the lifetime of the IKE security association times out.
A new SA must be negotiated before the current SA expires.
Because the negotiation about the IPSec security association is based on the IKE security association, a long lifetime should be configured for the IKE security association in order to save the time taken to negotiate about the IPSec security association. However, the longer the lifetime of the association, the more likely it will be cracked. Therefore, an appropriate lifetime (such as half a day) should be set as required.

Configuration Examples

The following example sets the lifetime of the IKE security association to 1000 seconds.

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# lifetime 1000
```

Related Commands

Command	Description
crypto isakmp enable	Enables IKE.
encryption { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }	Specifies an encryption algorithm.
hash { **sha** | **md5** | **sm3** }	Specifies the HASH algorithm.
authentication { **pre-share** | **rsa-sig** }	Specifies an authentication method.
group { **1** | **2** }	Specifies a Diffie-Hellman group ID.

Platform Description

N/A

match address (IPSec)

Use this command to specify an ACL for the crypto map entry in crypto map configuration mode.
Use the **no** form of this command to remove the ACL from the crypto map entry.
match address *access-list-number*

no match address

Parameter Description

Parameter	Description
access-list-number	ACL number (in the range from 100 to 199, from 2000 to 2699, and from 2900 to 3899). The crypto map only uses the extended IP ACL.

Defaults

No ACL is specified for the crypto map entry by default.

Command Mode

Crypto map configuration mode

Usage Guide

Use this command to specify an ACL for the crypto map entry. The crypto map entry uses the ACL to determine what data should be protected by IPSec.
The ACL specified through this command is used for both incoming and outgoing traffic. For

outgoing traffic, if matched data is detected and a security association exists, the data is encrypted and forwarded. If no security association is established, the security association negotiation (IKE) will be triggered. For incoming traffic, if matched data is detected and the data is encrypted, it will be decrypted. If the data is not encrypted, it will be discarded directly.

Configuration Examples

The following example associates the ACL 101 on the crypto map named mymap.

```
Ruijie(config)# crypto map mymap 4 ipsec-isakmp
Ruijie(config-crypto-map)# match address 101
```

Related Commands

Command	Description
crypto map (global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map (interface IPSec)	Associates the crypto map on an interface.

Platform Description

N/A

match any (IPSec-Profile)

Use this command when you need to specify the ACL for IKE negotiation as permit any.

match any

no match any

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No permit any ACL for IKE negotiation is specified for the crypto map entry by default.

Configuration Mode

Crypto map configuration mode

Usage Guide

Use this command to initiate and accept the permit any ACL during negotiation of IPV6, IPSEC-IPV4, and IPSEC-IPV6 tunnels.

The profile map configured with match any can be used only for IPIP and IPv6 tunnels; otherwise, configuration will fail. This occurs in the following conditions:

4) Match any is configured for the profile map, which is configured on non-IPIP and non–IPv6 tunnels. This causes configuration failure.
5) Match any is configured for the profile map, which is configured on the IPIP or IPv6 tunnel. After the tunnel mode is changed to non-IPIP or non-IPv6, the map configuration on the

tunnel interface is removed.

6) Match any is not configured for the profile map, which is applied to non-IPIP and non–IPv6 tunnels. This causes a failure in running the match any command.

Configuration Examples

The following example associates the ACL 101 on the crypto map named **mymap**.

```
Ruijie(config)# crypto map mymap 4 ipsec-isakmp
Ruijie(config-crypto-map)# match address 101
```

Related Commands

Command	Description
crypto ipsec profile *profile-name* **(global IPSec-Profile)**	Defines a tunnel crypto map entry.
tunnel protection ipsec profile [	N/A
show crypto map	Displays information about the crypto map.

Platform Description

N/A

match ipv6

Use this command to specify an IPv6 ACL for the crypto map entry in crypto map configuration mode.

Use the **no** form of this command to remove the IPv6 ACL from the crypto map entry.

match ipv6 *ipv6-acl-name*

no match ipv6

Parameter Description

Parameter	Description
ipv6-acl-name	IPv6 ACL name. The crypto map only uses the extended IP ACL.

Defaults

No IPv6 ACL is specified for the crypto map entry by default.

Command Mode

Crypto map configuration mode

Usage Guide

Use this command to specify an ACL for the crypto map entry. The crypto map entry uses the ACL to determine what data should be protected by IPSec.

The ACL specified through this command is used for both incoming and outgoing traffic. For outgoing traffic, if matched data is detected and a security association exists, the data is encrypted and forwarded. If no security association is established, the security association negotiation (IKE) will be triggered. For incoming traffic, if matched data is detected and the data is encrypted, it will be decrypted. If the data is not encrypted, it will be discarded directly.

Configuration

The following example associates the IPv6 ACL on the crypto map named mymap.

Examples

```
Ruijie(config)# crypto map mymap 4 ipsec-isakmp
Ruijie(config-crypto-map)# match address ipv6-acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

match vrf

Use this command to correlate the access list of crypto mapping entries with VRF.
Use the **no** form of this command to delete the correlation between the access list of crypto mapping entries and VRF.
match vrf *vrf-name*

no match vrf

Parameter Description

Parameter	Description
vrf-name	Name of VRF

Defaults

No VRF is assigned to the access list of crypto mapping entries

Command Mode

Crypto transform configuration mode

Usage Guide

Use this command to correlate the access list of crypto mapping entries with VRF. Only when the packets under the VRF matching the access list can they be protected by IPSec.

Configuration Examples

The following example correlates the access list of crypto mapping entries named mymap with VRF.

```
Ruijie(config)# crypto map mymap 4 ipsec-isakmp
Ruijie(config-crypto-map)# match vrf VRFA
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines the crypto map entry.
show crypto map	Display the crypto map entry
crypto map(interface IPSec)	Correlates the crypto map entry on the interface

Platform Description

N/A

mode (IPSec)

Use this command to change the mode of the crypto transform set in crypto transform configuration mode.
Use the **no** form of this command to restore the default mode.
mode { **tunnel** | **transport** }

no mode

Parameter Description

Parameter	Description
tunnel | **transport**	Specifies the mode of a transform set: tunnel or transport.

Defaults

A transform set is in tunnel mode by default.

Command Mode

Crypto transform configuration mode

Usage Guide

Mode setting takes effect only for the communications where both the source and destination addresses are IPSec peer (all other communications are performed in tunnel mode).
If the communication to be protected has the same IP address as the IPSec peer, namely the source and destination IP addresses are the IPSec peer, and the transport mode is specified, then during negotiation, a router will request for the transport mode, but it accepts both the transport mode and the tunnel mode. If the tunnel mode is specified, the router will request for the tunnel mode and accepts this mode only.

Configuration Examples

The following example specifies the mode of a transform set to the tunnel mode.

```
Ruijie(config)# crypto ipsec transform-set  myset
Ruijie(cfg-crypto-trans)# mode tunnel
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines the crypto transform set.

Platform Description

N/A

netmask

Use this command to configure a subnet mask. Use the **no** form of this command to restore the default setting.

netmask *ipmask*

no netmask

Parameter Description	Parameter	Description
	ipmask	IPv4 subnet mask

Defaults No subnet mask is configured by default.

Command Mode config-isakmp-group mode

Usage Guide N/A

Configuration Examples The following example configures a subnet mask.

```
Router(config-isakmp-group)# netmask 255.255.255.0
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

network center

Use this command to configure a network open to the clients. Use the **no** form of this command to restore the default setting.

network center *net-addr/prefix*

no network center *net-addr/prefix*

Parameter Description	Parameter	Description
	net-addr/prefix	IPv4 address or prefix (5 max)

Defaults No IPv4 address or prefix is configured by default.

Command Mode config-isakmp-group mode

Usage Guide N/A

Configuration Examples The following example configures a network open to the clients.

```
Router(config-isakmp-group)#network center 192.168.52.0/24
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

pool

Use this command to configure an address pool from which an IP address is selected for delivering a policy to a client. Use the **no** form of this command to restore the default setting.

pool *pool-name*

no pool

Parameter Description	**Parameter**	**Description**
	pool-name	Address pool name.

Defaults No address pool is configured by default.

Command Mode config-isakmp-group mode

Usage Guide The address pool is an IKE address pool.

Configuration Examples The following example configures an address pool.

```
Router(config-isakmp-group)# pool local-pool
```

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

Platform Description N/A

reverse-route

Use this coomand to enable reverse route injection
With reverse route injection enabled, the IPSec module automatically adds a static route after tunnel negotiation pointing to the tunnel peer, or specifies an IP address.
everse-route [**remote-peer** *ip-address*] [*distance*] [**tag** *tagvalue*] [**track** *trackvalue*] [**bfd**] [**weight** weightvalue]
no reverse-route

Parameter Description	**Parameter**	**Description**
	ip-address	(Optional) Next hop address
	distance	Next hop distance
	Tagvalue	Tag identifier of a route

trackvalue	Track identifier of a route
bfd	BFD route
weightvalue	Route weight

Defaults Reverse route injection is disabled by default.

Command Mode Crypto map configuration mode

Usage Guide You can run the **show ip route** command to view the added route.
You can run the **debug crypto ipsec** command to view the process of adding and deleting the reverse routes corresponding to tunnels.

Configuration Examples The following example enables reverse route injection.

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# reverse-route
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines the crypto map entry.
debug crypto ipsec	IPSec sa debgging information

Platform Description N/A

reverse-ipv6-route

Use this coomand to enable IPv6 reverse route injection. With reverse route injection enabled, the IPSec module automatically adds a static route after tunnel negotiation pointing to the tunnel peer, or specifies an IP address. Use the **no** form of this command to restore the default configuration.

reverse-ipv6-route [**remote-peer** *ip-address*] [*distance*] [**bfd**] [**weight** *weightvalue*]

no reverse-route

Parameter Description

Parameter	Description
ip-address	(Optional) Next hop address
distance	Next hop distance
bfd	BFD route
weightvalue	Route weight

Defaults IPv6 reverse route injection is disabled by default.

Command Mode Crypto map configuration mode

Usage Guide

You can run the **show ip route** command to view the added route.
You can run the **debug crypto ipsec** command to view the process of adding and deleting the reverse routes corresponding to tunnels.

Configuration Examples

The following example enables IPv6 reverse route injection.

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# reverse-ipv6-route
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

self-identity

Use this command to specify the form of the self-identity.

self-identity { **address** | **trustpoint** *trustpoint* | **fqdn** *fqdn* | **user-fqdn** *user-fqdn* }

no self-identity

Parameter Description

Parameter	Description
address	Local IP address
trustpoint	Default certificate chain set at the local end
fqdn	Domain name set at the local end
user-fqdn	User name and domain name set at the local end

Defaults

The address parameter is set to the local IP address by default.

Command Mode

Global configuration mode

Usage Guide

This command is mainly used to set the identity in the negotiation initiated in aggressive mode. The self-identity can be specified by either a domain name or an address.

Configuration Examples

The following example sets the identity.

```
Ruijie(config)# self-identity fqdn www.vpdn.com
Ruijie(config)# self-identity user-fqdn
zj@www.vpdn.com
Ruijie(config)# self-identity address
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

set autoup

Use this command to set automatic tunnel connection in crypto map configuration mode. Generally, the IPSec tunnel is triggered by packets. After this command is ececuted, the tunnel will be triggered by the IPSec module.

set autoup

no set autoup

Parameter Description

Parameter	Description
N/A	N/A

Defaults Automatic tunnel connection is disabled by default.

Command Mode Crypto map configuration mode

Usage Guide This function avoids packet loss due to tunnel negotiation. It is sentitive to data transmission and must be used when tunnels are always in the UP state.

Configuration Examples

The following example sets the working mode (aggressive mode).

```
Ruijie(config)# crypto map mymap 10 ipsec-isakmp
Ruijie(config-crypto-map)# set autoup
```

Related Commands

Command	Description
crypto map(interface IPSec)	Applies the crypto map to an interface.
match address	Specifies an ACL for the crypto map list.
set peer	Specifies a remote peer.
set transform-set	Specifies a transform set.
show crypto map	Displays information about the crypto map.

Platform Description	N/A

set exchange-mode

Use this command to set the working mode for the first stage during IKE negotiation between peers.

set exchange-mode { **main** | **aggressive** }

no set exchange-mode

Parameter Description

Parameter	Description
main	Main mode
aggressive	Aggressive mode

Defaults The main mode is used by default.

Command Mode Crypto map configuration mode

Usage Guide

There are two stages during IKE negotiation:
The first stage - establishes a secure and authenticated channel for communication between two ISAKMP entities. The main mode and aggressive mode are used in this stage.
The second stage - negotiates about the security association that represents the service.
There are two working modes in the first stage. Based on their advantages and disadvantages, the main mode is used by default. However, the aggressive mode can be used when the IP address is not fixed.

Configuration Examples

The following example sets the working mode (aggressive mode).

```
Ruijie(config)# crypto map mymap 10 ipsec-isakmp
Ruijie(config-crypto-map)# set exchange-mode
aggressive
```

Related Commands

Command	Description
crypto map(interface IPSec)	Applies the crypto map to an interface.
match address	Specifies an ACL for the crypto map list.
Set peer	Specifies a remote peer.
Set transform-set	Specifies a transform set.
show crypto map	Displays information about the crypto map.

Platform Description N/A

set local (IPSec)

Use this command to specify the local IP address in the crypto map entry in crypto map configuration mode.
Use the **no** form of this command to remove the remote peer from the crypto map entry.
set local *ip-address*

no set local *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address used at the local end

Defaults No remote peer is specified by default.

Command Mode Crypto map configuration mode

Usage Guide Use this command to configure the IP address for the negotiation at the local end. If this command is not executed, the main interface address is used for negotiation. If this command is executed, the configured IP address is used for negotiation.

Configuration Examples The following example specifies a remote peer (2.2.2.2) for the crypto map named **mymap**.

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set local 2.2.2.2
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines the crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.

Platform Description N/A

set mtu

Use this command to set the MTU. Use the **no** form of this command to remove the remote peer from the crypto map entry.

set mtu *length*

no set mtu

Parameter Description

Parameter	Description
length	Sets the MTU, in the range from 512 to 1500.

Defaults No MTU is set by default.

Command Mode Crypto map configuration mode

Usage Guide N/A

Configuration The following example sets the MTU to 1000.

Examples

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set mtu 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

set peer (IPSec)

Use this command to specify a remote peer in the crypto map entry in crypto map configuration mode.

Use the **no** form of this command to remove the remote peer from the crypto map entry.

set peer { *hostname* | *ip-address* } [*trustpoint1* [*trustpoint2* [*trustpoint3*]]]

no set peer { *hostname* | *ip-address* }

Parameter Description

Parameter	Description
ip-address	IP address of the remote peer
hostname	Host name of the remote peer
trustoint1	Certificate chain at this segment
trustpoint2	Certificate chain at the peer end
trustpoint3	Use crypto certificate at this segment. Special for version 2014 digital envelope certification.

Defaults

No remote peer is specified by default.

Command Mode

Crypto map configuration mode

Usage Guide

A remote peer must be specified for the crypto map in use.

When multiple local certificate chains exist, certificate chains are specified based on each peer. When no local certificate chain is specified, the ca certificate at the peer end is used for authentication. When no peer certificate chain is specified, the default ca certificate is used for authentication.

Configuration Examples

The following example specifies a remote peer (2.2.2.2) for the crypto map named mymap.

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set peer 2.2.2.2
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines a crypto map entry.

show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.

Platform Description N/A

set pfs (IPSec)

Use this command to specify the Diffie-Hellman group identifier for IPSec tunnel encapsulation.

set pfs { **group1 | group2| group5** }

no set pfs

Parameter Description

Parameter	Description
group1	768 bits
group2	1024 bits
group5	1536 bits

Defaults No Diffie-Hellman group is used by default.

Command Mode Crypto map configuration mode

Usage Guide Use this command to specify the Diffie-Hellman group identifier for IPSec tunnel encapsulation.

Configuration Examples The following example specifies the 1024-bit Diffie-Hellman for the crypto map named **mymap**.

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set pfs group2
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.

Platform Description N/A

set security-association idle-time

Use this command to configure automatic disconnection for idle tunnels. Use the **no** form of this command to remove the default configuration.

set security-association idle-time *sec*

no set ipsec security-association idle-time

Parameter Description

Parameter	Description
sec	Tunnel idle time (in seconds)

Defaults

The tunnel is not torn down automatically by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to tear down the tunnel when the idle time expires. After this command is configured, the global idle time is not valid for this tunnel.

Configuration Examples

The following example sets the idle time to 120 seconds.

```
Ruijie(config)# crypto map map-name seq-num
ipsec-isakmp
Ruijie(config-crypto-map)# set security-association idle-time 120
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

set security-association lifetime

Use this command to replace a certain crypto map to negotiate the global lifetime of the IPSec security association in crypto map configuration mode.
Use the **no** form of this command to restore the default value.
set security-association lifetime { **seconds** *seconds* | **kilobytes** *kilobytes*] }

no set security-association lifetime { **seconds** | **kilobytes** }

Parameter Description

Parameter	Description
seconds *seconds*	Timeout value (in seconds) of the security association
kilobytes *kilobytes*	Timeout communication volume (in kilobytes) of the security association

Defaults

The security association of the crypto map is negotiated based on the global lifetime value by default.

Command Mode

Crypto map configuration mode

Usage Guide

This command only applies to the crypto map whose IPSec security association is established using IKE. This command is not available to the crypto map whose security association is

established manually.

By default, all IPSec security associations are negotiated using the global lifetime value. If a lifetime different from the global lifetime value should be used for a certain destination IP address, you can use this command to change the lifetime value in the crypto map entry that negotiates with this destination IP address.

Note

Changing the lifetime value with this command only changes the lifetime value for a specific map to negotiate the IPSec security association, and has no impact on the global lifetime value.

Configuration Examples

The following example changes the lifetime of entry 5 of the crypto map named **mymap** to 2500 seconds.

```
Ruijie(config)# crypto map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set security-association lifetime seconds 2500
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.
crypto ipsec security-association lifetime	Configures the global lifetime.

Platform Description

N/A

set session-key

Use this command to configure the security parameter index (SPI) and password of the algorithm related to the protected incoming and outgoing communication when you need to establish a security association manually.

Use the **no** form of this command to remove the SPI and password of the related algorithm.

set session-key { **inbound** | **outbound** } **ah** *spi hex-key-data*

set session-key { **inbound** | **outbound** } **esp** *spi* **cipher** *hex-key-data* [**authenticator** *hex-key-data*]

no set session-key { **inbound** | **outbound** } **ah**

no set session-key { **inbound** | **outbound** } **esp**

Parameter Description

Parameter	Description
spi	SPI
hex-key-data	Password in hexadecimal notation

Defaults The SPI and password of the related algorithm are not specified by default.

Command Mode Crypto map configuration mode

Usage Guide This command is used only in IPSec-manual.

Configuration Examples

The following example configures the passwords of esp encapsulation and decapsulation for the crypto map named **mymap**.

```
Ruijie(config)# crypto map mymap 5 ipsec-manual
Ruijie(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
Ruijie(config-crypto-map)# set session-key outbound esp 300 cipher abcdef1234567890
```

Related Commands

Command	Description
crypto map(global IPSec) ipsec-manual	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.

Platform Description N/A

set transform-set

Use this command to specify the transform sets to be used for a certain crypto map entry in crypto map configuration mode.

Use the **no** form of this command to remove the association between the crypto map entry and the transform set.

Set transform-set *transform-set-name1* [*transform-set-name2*] [*transform-set-name3*] [*transform-set-name4*] [*transform-set-name5*] [*transform-set-name6*]

no set transform-set

Parameter Description

Parameter	Description
transform-set-name1, [*transform-set-name2*], [*transform-set-name3*], [*transform-set-name4*], *[transform-set-name5]*, *[transform-set-name6]*	Name of the transform set. Up to six transform sets can be specified for a crypto map entry.

Defaults No transform set is specified by default.

Command Mode Crypto map configuration mode

Usage Guide Transform sets are necessary to establish the security association successfully. You must use this command to specify a transform set when configuring any crypto map.

Configuration Examples The following example specifies the transform set for the crypto map entry as **myset**.

```
Ruijie(config)# crypto ipsec transform-set myset  esp-des esp-sha-hmac
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set transform-set myset
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.

Platform Description N/A

set vrf

Use this command to correlate crypto mapping entries with VRF.

set vrf *vrf-name*
no set vrf

Parameter Description

Parameter	Description
vrf-name	Name of the VRF

Defaults No VRF switch is specified by default.

Command Mode Crypto map configuration mode

Usage Guide Use this command to correlates the IPSec tunnel with designated VRF.

Configuration Examples The following example correlates crypto mapping entries with VRF .

```
Ruijie(config)# crypto ipsec transform-set myset  esp-des esp-sha-hmac
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set vrf VRFA
```

Related

Command	Description

Commands

crypto map(global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.

Platform Description N/A

set mtu

Use this command to set the pre-fragment mode for IPSec (effective for the tunnel mode).

set mtu *length*

no set mtu

Parameter Description

Parameter	Description
length	Packet fragment size before encapsulation, in the range from 512 to 1500

Defaults The pre-fragment mode is not used by default.

Command Mode Crypto map configuration mode

Usage Guide Use this command to set the pre-fragment mode for IPSec tunnel encapsulation.

Configuration Examples The following example sets the pre-fragment mode for the crypto map named **mymap**.

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# set mtu 1000
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.
crypto map(interface IPSec)	Associates the crypto map on an interface.

Platform Description N/A

tunnel protection ipsec profile (interface IPSec for IPSec-Profile)

Use this command to apply a predefined profile crypto map set to a tunnel interface in interface configuration mode.

Use the **no** form of this command to remove the association of the crypto map set on an interface.

tunnel protection ipsec profile [*profile-name*]

no tunnel protection ipsec profile [*profile-name*]

Parameter Description

Parameter	Description
profile-name	Name of the profile crypto map

Defaults

No crypto map is applied to tunnel interfaces.

Command Mode

Interface configuration mode

Usage Guide

Use this command to apply a crypto map set to an interface, which is required to perform IPSec encryption and protection on all packets on tunnel interfaces. Each interface can be associated with only one crypto map set.


Note

Profile maps can only be configured on GRE, IPIP, and IPv6 tunnels. When profile maps are configured on other tunnels, configuration will fail. When the tunnel mode is changed to a mode that is not supported by profile maps, the profile maps on tunnel interfaces will be removed.

Configuration Examples

The following example applies the crypto map named **profile-name** to the interface Tunnel 1.

```
Ruijie(config)# interface  tunnel  1
Ruijie(config-if-Tunnel 1) # tunnel protection ipsec profile profile-name
```

Related Commands

Command	Description
crypto map(global IPSec)	Defines a crypto map entry.
show crypto map	Displays information about the crypto map.

Platform Description N/A

username password

Use this command to configure a username and a password. Use the **no** form of this command to remove the default configuration.

username *name* **password { 0 | 7 }** *pass*

no username

Parameter Description

Parameter	Description
name	Username
pass	Password

Defaults No username or password is configured.

Command Mode Crypto map configuration mode

Usage Guide After this command is configured, the IKE initiator initiates IKE negotiation by using extended authentication.

Configuration Examples The following example configures a username and a password.

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show crypto dynamic-map (IPSec)

Use this command to view information about the dynamic crypto map in privileged EXEC mode.

show crypto dynamic-map [***map-name***]

Parameter Description

Parameter	Description
map-name	Name of a crypto map

Defaults If the name of a crypto map is not specified, information about all dynamic crypto maps on a router is displayed.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# show crypto dynamic-map
      Crypto Map Template "mydmap" 1
No matching address list set.
Security association lifetime: 4608000 kilobytes/3600 seconds(id=34)
PFS (Y/N): N
Transform sets = {  }
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show crypto ipsec sa

Use this command to view details about the currently active IPSec security association in privileged EXEC mode.

show crypto ipsec sa

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 an output of this command.

```
Interface: GigabitEthernet 1/0/0
```

```
       Crypto map tag:mymap, local addr 2.2.2.3
//The current crypto map set is named mymap and uses the local address
2.2.2.2.
media mtu 1500
       ================================
       sub_map type:static, seqno:7, id=0
       local  ident (addr/mask/prot/port): (2.2.2.3/0.0.0.0/0/0))
       remote  ident (addr/mask/prot/port): (2.2.2.2/0.0.0.0/0/0))
PERMIT
//Protect the communication between 2.2.2.3 and 2.2.2.2.
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
       #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
       #send errors 0, #recv errors 0
//Statistics in the following order: number of encapsulated packets, number
of encrypted packets, number of digest packets, number of decapsulated
packets, number of decrypted packets, number of verification packets, send
errors, and receive errors
inbound esp sas:
//Security association for incoming packet processing, with the protocol
ESP
spi:0x79b8e4bb (2042160315)
//The value of spi is 2042160315.
transform: esp-3des
//The transform set is esp-3des.
in use settings={Tunnel,}
//Tunnel mode
crypto map mymap 7
sa timing: remaining key lifetime (k/sec): (4607000/3505)
//There are 4607000 kbytes and 3505 seconds left before the lifetime of
the security association is reached.
IV size: 8 bytes
//The IV vector length is 8.
max reply windows size: 0
Replay detection support:Y
//Anti-replay processing



outbound esp sas:
//Security association for outgoing packet processing, with the protocol
ESP
spi:0x293b8b55 (691768149)
//The value of spi is 691768149.
transform: esp-3des
//The transform set is esp-3des.
in use settings={Tunnel,}
```

```
//Tunnel mode
crypto map mymap 7
            sa timing: remaining key lifetime (k/sec): (4607000/3505)
//There are 4607000 kbytes and 3505 seconds left before the lifetime of
the security association is reached.
IV size: 8 bytes
//The IV vector length is 8.
max reply windows size: 0
            Replay detection support:Y
//Anti-replay processing
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show crypto ipsec transform-set

Use this command to view information about the transform set configured on a router in privileged EXEC mode.

show crypto ipsec transform-set

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 an output of this command.

```
Ruijie#show crypto ipsec transform-set
transform set myset3: { esp-des,}
      will negotiate = {Tunnel,}
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

show crypto isakmp policy

Use this command to view the IKE policy information configured on a router in privileged EXEC mode.

show crypto isakmp policy

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 an output of this command.

```
Ruijie# show crypto isakmp p
Protection suite of priority 9
encryption algorithm:   3DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Message Digest 5
authentication method:  Pre-Shared Key
Diffie-Hellman group:   #2 (1024 bit)
lifetime:             1000 seconds
Protection suite of priority 10
encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Message Digest 5
authentication method:  Pre-Shared Key
Diffie-Hellman group:   #2 (1024 bit)
lifetime:             1000 seconds
Default protection suite
encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Secure Hash Standard
authentication method:  Rsa-Sig
Diffie-Hellman group:   #1 (768 bit)
lifetime:             86400seconds
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

show crypto isakmp sa

Use this comand to view the currently active IKE security associations on a router in privileged EXEC mode.

show crypto isakmp sa

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 an output of this command.

```
Ruijie#!!show crypto  isakmp sa!
 destination   source    state    conn-id   lifetime(second)
 1.1.1.1       1.1.1.2  IKE_IDLE  59        32254
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show crypto map (IPSec)

Use this command to query information about the crypto map in privileged EXEC mode.

show crypto map [*map-name*]

Parameter Description

Parameter	Description
map-name	Name of a crypto map

Defaults

If the name of a crypto map is not specified, information about all the crypto maps on a router will be displayed.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example shows an output of this command.

```
Ruijie#show crypto map

Crypto Map:"mymap1" 1 ipsec-isakmp, (Complete)
       Extended IP access list 100
       Security association lifetime: 0 kilobytes/120 seconds(id=2)
       PFS (Y/N): N
       Transform sets = { myset3,  }

       Interfaces using crypto map mymap1:
              GigabitEthernet 1/1/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Digital Certificate Commands

certificate

Use this command to manually add a certificate in certificate chain configuration mode (config-cert-chain).
Use **no** form of this command to remove the certificate.
certificate [**ca**] *certificate-serial-number*
no certificate [**ca**] *certificate-serial-number*

Parameter Description

Parameter	Description
ca	CA certificate
certificate-serial-number	Serial number of the certificate to be added or deleted

Defaults N/A

Command Mode Certificate chain configuration mode (config-cert-chain)

Usage Guide You can use this command to manually define a certificate, but such usage is quite rare. This command is generally used to paste or delete a certificate.

Configuration Examples The following example deletes the router certificate. The example uses a show command to display the serial number of the certificate to be deleted.

```
Ruijie# show crypto pki certificate
...,...
%Router certificate info:
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
16:2a:7a:1d:00:00:00:00:00:02
Signature Algorithm: sha1WithRSAEncryption
...,...
Ruijie# config t
Ruijie(config)# crypto pki certificate chain
Ruijie(config-cert-chain)# no certificate 162a7a1d000000000002
Ruijie(config-cert-chain)# exit
Ruijie(config)#
```

Related

Command	Description

Commands		
	crypto pki certificate chain	Certificate chain configuration command

Platform Description N/A

crypto pki authenticate

When you use the SCEP protocol to acquire the router certificate, run this command to acquire the root certificate of CA in global configuration mode.

crypto pki authenticate *ca_name*

Parameter Description	Parameter	Description
	ca_name	Common name of the CA corresponding to a trust point

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

```
router(config)#crypto pki authenticate CA
Certificate has the following attributes:
MD5 fingerprint: B4DE1DD7 E9902423 5E6330D7 D750A432
SHA1 fingerprint: AD070162 672A7C57 BD5EE522 A95AAFA1 351524D0
% Do you accept this certificate?[yes/no]:yes    //Select yes to accept the
CA certificate
Trustpoint CA certificate accepted.
```

Related Commands	Command	Description
	crypto pki trustpoint	Configures a trust point.

Platform Description N/A

crypto pki certificate chain

Use this command to enter certificate chain configuration mode (config-cert-chain) in global configuration mode (you can delete a certificate only in certificate chain configuration mode).

Use the **no** form of this command to delete a certificate chain and all its certificates.

crypto pki certificate chain *ca_name*
no crypto pki certificate chain *ca_name*

Parameter Description

Parameter	Description
ca_name	Common name of the CA corresponding to a trust point

Defaults N/A

Command Mode Global configuration mode

Usage Guide You can use this command to enter certificate chain configuration mode. In this mode, you can configure or delete a certificate. If you run the **no crypto pki certificate chain** command, all certificates in the certificate chain will be deleted.

Configuration Examples The configuration example here is the same as that of the **certificate** command.

Related Commands

Command	Description
certificate	Manual certificate configuration

Platform Description N/A

crypto pki certificate peer

Use this command to import the certificate file of the peer device. This command is specially developed for digital envelop authentication. During digital envelope authentication, the certificate will be located first based on the peer address before negotiation is initiated.
crypto pki certificate peer *ip_address*

Parameter Description

Parameter	Description
ip_address	IP address of the peer device

Defaults N/A

Command Mode Global configuration mode

Usage Guide The process is the same as that of importing certificates: directly Paste the pem formatted file of the certificate.

crypto pki certificate peer address 192.168.50.203 //IP address of the peer device

% Enter PEM-formatted peer certificate.
% End with a blank line or "quit" on a line by itself.
//Paste the certificate of the peer
quit
import peer certificate success.

Configuration Examples

```
Router(config)#crypto pki certificate peer address 192.168.50.203  //IP address of the peer device

% Enter PEM-formatted peer certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIDLjCCAtigAwIBAgIQVq4HPBChfoxFro0/FVIzVzANBgkqhkiG9w0BAQUFADCB
rDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0LmNuMQswCQYDVQQGEwJD
TjEPMA0GA1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpob3UxIDAeBgNVBAoTF1Jl
Z2lhbnQgTmV0d29yayBDby4gTHRkMR0wGwYDVQQLExRSZXNlYXJjaCBBcGFydG1l
bnQgNTEXMBUGA1UEAxMOQ0EgdGVzdCBzZXJ2ZXIwHhcNMDUwMjI1MDg0NjAyWhcN
MDcwMzAxMDIzNjIzWjCBrDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0
LmNuMQswCQYDVQQGEwJDTjEPMA0GA1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpo
b3UxIDAeBgNVBAoTF1JlZ2lhbnQgTmV0d29yayBDby4gTHRkMR0wGwYDVQQLExRS
ZXNlYXJjaCBBcGFydG1lbnQgNTEXMBUGA1UEAxMOQ0EgdGVzdCBzZXJ2ZXIwXDAN
BgkqhkiG9w0BAQEFAANLADBIAkEA2R8axg75UZJM3JZNREP62r5T8t31E7Y0taah
n/1XoWxvevShE8FZPQxMPo5i3nbYokzyLPjagqoX0+jMgMKVjwIDAQABo4HTMIHQ
MAsGA1UdDwQEAwIBxjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRyQ4QcKwNF
LYJY9YRDd/UhqkssITB/BgNVHR8EeDB2MDigNqA0hjJodHRwOi8vemotcm91dGVy
L0NlcnRFbnJvbGwvQ0ElMjB0ZXN0JTIwc2VydmVyLmNybDA6oDigNoY0ZmlsZTov
L1xcemotcm91dGVyXENlcnRFbnJvbGxcQ0ElMjB0ZXN0JTIwc2VydmVyLmNybDAQ
BgkrBgEEAYI3FQEEAwIBATANBgkqhkiG9w0BAQUFAANBAH8ufRZ2tVYO3R7YC0IF
OzmnQrjgaBN4bpmSLkxYYKtK8ZNjo0FwUL11aq6nCGp6n8Ks0dijoMxnedB2zn0a
f0w=
-----END CERTIFICATE-----
quit
import peer certificate success.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

crypto pki crl request

Run this command to manually download a CRL file in global configuration mode.

This command does not have the **no** form.

crypto pki crl request *trustpoint*

Parameter Description

Parameter	Description
trustpoint	Specifies the trust point certificate chain.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command cannot be saved. RGOS can support up to 1 MB CRL file size, and will deny the download of files exceeding that size. RGOS supports the download of CRL files through HTTP. The URL can be obtained by the following means (by order of precedence):

1. Specified through the command line, such as **crypto pki crl url** *http://www.myca.cn/CertEnroll/certcrl.crl*
2. Extension of the CRL distribution point of the CA root certificate configured on a device
3. Extension of the CRL distribution point of the router certificate configured on a device

For information about URL, see the usage guide of the **crypto pki crl url** command.

Configuration Examples The following example displays the execution process and result of this command. **certcrl.crl** is a CRL file.

```
Ruijie# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# crypto pki crl request trustpoint
%Crypto pki crl request command: start crl download task!
Ruijie(config)#
%Crl download and decode successfully!
Ruijie(config)# exit
Ruijie#dir
Directory of flash:/
5    an      68 0xdbc28957 Jan  1 2005 00:00:00 tftp_config.bin
8    an  4301816 0x3e415b47 Jun 28 2005 15:03:46 RGOS.bin
27    an    5331 0xaf1d58ec Jun 29 2005 10:05:20 config.text
34    an     427 0x5bd43f32 Jun 29 2005 12:50:41 certcrl.crl
```

Related Commands

Command	Description
crypto pki crl url	Specifies the URL for downloading a CRL file.

Platform Description N/A

crypto pki crl url

Use this command to specify the URL for downloading a CRL file in global configuration mode.
Use the **no** form of this command to delete this address.
The configuration of this command is the same as the CRL configruation of the first certification chain and is introduced only to keep compatible with earlier versions.
crypto pki crl url *url_string*
no crypto pki crl url

Parameter Description

Parameter	Description
url_string	URL character string starting with http://, with length not exceeding 255

Defaults N/A

Command Mode Global configuration mode

Usage Guide If this command is not executed, RGOS can still obtain the CRL download address from the CRL distribution point information of the CA root certificate or router certificate. When this command is executed, the configuration of this command is preferred. That is, the address in the certificate will not be used.
url_string must begin with http://. The download port will use port 80 by default; otherwise, you must specify the port behind the domain name, such as http://www.myca.cn:1020/. The directory name is **certsrv** by default, or you can specify the directory name separately, such as http://www.myca.cn/CertDir/. The CRL file name is **certcrl.crl** by default, or you can specify the CRL file name separately, such as http://www.myca.cn/certsrv/mycertcrl.crl. *url_string* must contain no space. If your URL must contain space, you can type in **%20** instead, such as http://www.myca.cn/CertEnroll/CA%20Server.crl.
The domain name of *url_string* can use an IP address directly, such as http://202.101.211.123/, or an internal host name, such as http://myserver/. No matter whether the URL is obtained through manual configuration or from a certificate, a device will automatically proceed with domain name resolution or host name resolution when starting to download a CRL file. Ensure that the relevant configurations are correct. If domain name resolution is required, the correct DNS address must be configured. If internal host name resolution is required, use the **ip host** command to configure the IP address of the host.

Configuration The following example displays valid configurations of this command.

Examples

```
http://www.myca.cn/certsrv/certcrl.crl
http://www.myca.cn:1010/certsrv/
http://www.myca.cn:80/certsrv
http://www.myca.cn/certcrl.crl
http://www.myca.cn:80/
http://www.myca.cn:1220
http://www.myca.cn
http://www.myca.cn/CertEnroll/CA%20Server.crl
http://202.101.211.123/certsrv/certcrl.crl
```

Related Commands

Command	Description
crypto pki crl request	Manually downloads a CRL file.

Platform Description N/A

crypto pki enroll

Use this command to perform enrollment in global configuration mode when you use the SCEP protocol to acquire the router certificate.

crypto pki enroll *ca_name*

Parameter Description

Parameter	Description
ca_name	Common name of the CA corresponding to a trust point

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples router(config)#crypto pki enroll CA

```
%
%Start certificate enrollment ..
%Create a challenge password. You will need to verbally provide this password
to the CA Administrator in order to revoke your certificate. For security reasons
your password will not be saved in the configuration.Please make a note of it.

Password:F4EEE4FEB3766007    //Enter the password obtained from the CA.
Re-enter password:F4EEE4FEB3766007
```

```
%The subject name in the certificate will include: router
```

Related Commands	Command	Description
	crypto pki trustpoint	Configures a trust point.

Platform Description N/A

crypto pki import crl

Use this command to import a CRL file through TFTP in global configuration mode.
This command does not have the **no** form.
crypto pki import ***c****a_name* **crl** *tftp_url*

Parameter Description	Parameter	Description
	ca_name	Common name of the CA corresponding to a trust point
	terminal	Manually imports certificates and keys from the console terminal.
	tftp_url	TFTP URL of the CRL file

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command cannot be saved. You can use this command to import certificates and RSA key pairs from PEM-formatted files, which may come from other PKI application devices

Configuration Examples N/A

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

crypto pki import pem

Use this command to import certificates and keys from privacy-enhanced mail (PEM)-formatted files in global configuration mode.

This command does not have the **no** form.

crypto pki import *ca_name* **pem terminal** *password* [**id** *string*]

Parameter Description

Parameter	Description
ca_name	Common name of the CA corresponding to a trust point
terminal	Manually imports certificates and keys from the console terminal.
password	Password that is used to protect the keys during certificate export. Here it is used to decrypt the keys.
string	Special ID for Sm2 certification.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command cannot be saved. You can use this command to import certificates and RSA key pairs from PEM-formatted files, which may come from other PKI application devices such as PCs.

Configuration Examples The following example imports certificates and keys through this command.

```
Ruijie# config t
Ruijie(config)# crypto pki import ca_name pem terminal 12345678
% Enter PEM-formatted CA certificate.
```

//Prompts the user to enter the PEM-formatted CA root certificate text.

```
% End with a blank line or "quit" on a line by itself.  //Prompts the user to enter a blank line or type in quit to end text input.
```

//Copy the CA root certificate text and paste here, as shown below:

```
-----BEGIN CERTIFICATE-----
MIIDLjCCAtigAwIBAgIQVq4HPBChfoxFro0/FVIzVzANBgkqhkiG9w0BAQUFADCB
rDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0LmNuMQswCQYDVQQGEwJD
TjEPMA0GA1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpob3UxIDAeBgNVBAoTF1Jl
Z2lhbnQgTmV0d29yayBDby4gTHRkMR0wGwYDVQQLExRSZXNlYXJjaCBBcGFydG1l
bnQgNTEXMBUGA1UEAxMOQ0EgdGVzdCBzZXJ2ZXIwHhcNMDUwMjI1MDg0NjAyWhcN
MDcwMzAxMDIzNjIzWjCBrDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0
LmNuMQswCQYDVQQGEwJDTjEPMA0GA1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpo
b3UxIDAeBgNVBAoTF1JlZ2lhbnQgTmV0d29yayBDby4gTHRkMR0wGwYDVQQLExRS
ZXNlYXJjaCBBcGFydG1lbnQgNTEXMBUGA1UEAxMOQ0EgdGVzdCBzZXJ2ZXIwXDAN
BgkqhkiG9w0BAQEFAANLADBIAkEA2R8axg75UZJM3JZNREP62r5T8t31E7Y0taah
```

```
n/1XoWxvevShE8FZPQxMPo5i3nbYokzyLPjagqoX0+jMgMKVjwIDAQABo4HTMIHQ
MAsGA1UdDwQEAwIBxjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRyQ4QcKwNF
LYJY9YRDd/UhqkssITB/BgNVHR8EeDB2MDigNqA0hjJodHRwOi8vemotcm91dGVy
L0NlcnRFbnJvbGwvQ0ElMjB0ZXN0JTIwc2VydmVyLmNybDA6oDigNoY0ZmlsZTov
L1xcemotcm91dGVyXENlcnRFbnJvbGxcQ0ElMjB0ZXN0JTIwc2VydmVyLmNybDAQ
BgkrBgEEAYI3FQEEAwIBATANBgkqhkiG9w0BAQUFAANBAH8ufRZ2tVYO3R7YC0IF
OzmnQrjgaBN4bpmSLkxYYKtK8ZNjo0FwUL11aq6nCGp6n8Ks0dijoMxnedB2zn0a
f0w=
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
Fingerprint: B286A3F4 4930D46D 81D4A544 885D611C
```

//Fingerprint of the CA root certificate

```
% Do you accept this certificate? [yes/no]: yes
```

//Prompts the user to verify the fingerprint.

```
% Certificate successfully imported
% Enter PEM-formatted encrypted private key.
```

//Prompts the user to enter the PEM-formatted private key.

```
% End with "quit" on a line by itself.
```

//Prompts the user to type in **quit** to end text input.

//Copy the private key text and paste here, as shown below:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,251F9D955610C376

GDG2s1mbs/MJCpo5w2bu972jK1OZYtv3RQunH4I29c9H5uq3LtyvNA9RwrlpRQ3t
iUmkvQrU3/6SBp4Rqx1EU2UWgv1KRqqYwRVbdPdBZYVJLrso3Ov/9eaS4TiD+4Dl
NfJ1sAA4OONdVKDCLcGZIB43Wq5rAlqzsyjcF6tx3fWsSankVjQfroTv7UvP+ijj
uGndmJwbXEiATxlt+Smvt2/CGjr8nIC55T1W+tW0itkBdZhnvBJekOFM4BdgoLZc
3vueTIHmTurHvvdLIytYjQHsxVsf3vRGMcQhohM98nAYsIDBil4OIh1hc+ZnhGsn
TFLPMmMuJnBWMYopfaMPNrcdbpu+n4Qj2QiRoVTEoI7P1IAY/Oa2uc+kDuUX3KlW
sQQPnFNiU0Q/T9BrsolxI2Wkak7cvaNxbmhuU+5wNUGybQfcfP3CWg==
-----END RSA PRIVATE KEY-----
quit
% RSA private key successfully imported
Enter the base 64 encoded certificate.//Prompts the user to enter the
PEM-formatted router certificate text.
End with a blank line or the word "quit" on a line by itself
```

//Prompts the user to enter a blank line or type in **quit** to end text input

//Copy the router certificate text and paste here, as shown below:

```
-----BEGIN CERTIFICATE-----
MIIEsTCCBFugAwIBAgIKEffFFwABAAAAPjANBgkqhkiG9w0BAQUFADCBrDEhMB8G
CSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0LmNuMQswCQYDVQQGEwJDTjEPMA0G
A1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpob3UxIDAeBgNVBAoTF1JlZ2lhbnQg
TmV0d29yayBDby4gTHRkMR0wGwYDVQQLExRSZXNlYXJjaCBBcGFydG1lbnQgNTEX
```

```
MBUGA1UEAxMOQ0EgdGVzdCBzZXJ2ZXIwHhcNMDUwNDEyMDkyOTUzWhcNMDYwNDEy
MDkzOTUzWjCBpDEhMB8GCSqGSIb3DQEJARYSZGluZ2pzQHN0YXItbmV0LmNuMQsw
CQYDVQQGEwJDTjEPMA0GA1UECBMGRnVKaWFuMQ8wDQYDVQQHEwZGdVpob3UxIDAe
BgNVBAoTF1JlZ2lhbnQgTmV0d29yayBDby4gTHRkMR0wGwYDVQQLExRSZXNlYXJj
aCBBcGFydG1lbnQgNTEPMA0GA1UEAxMGZGluZ2pzMFwwDQYJKoZIhvcNAQEBBQAD
SwAwSAJBAM0sOymB/5v35vnf/PlJX+aqZpH9drtevsNaHkj4i3XdaJ55rFo2wLT0
qpWTI0nu638ktUa4dEIfF0AQM67sP0ECAwEAAaOCAmMwggJfMA4GA1UdDwEB/wQE
AwIE8DATBgNVHSUEDDAKBggrBgEFBQgCAjAdBgNVHQ4EFgQUIWVn8+ciY7JJkOFN
7MIkcRWWpx8wgegGA1UdIwSB4DCB3YAUckOEHCsDRS2CWPWEQ3f1IapLLCGhgbKk
ga8wgawxITAfBgkqhkiG9w0BCQEWEmRpbmdqc0BzdGFyLW5ldC5jbjELMAkGA1UE
BhMCQ04xDzANBgNVBAgTBkZ1Smlhbj EPMA0GA1UEBxMGRnVaaG91MSAwHgYDVQQK
ExdSZWdpYW50IE5ldHdvcmsgQ28uIEx0ZDEdMBsGA1UECxMUUmVzZWFyY2ggQXBh
cnRtZW50IDUxFzAVBgNVBAMTDkNBIHRlc3Qgc2VydmVyghBWrgc8EKF+jEWujT8V
UjNXMH8GA1UdHwR4MHYwOKA2oDSGMmh0dHA6Ly96ai1yb3V0ZXIvQ2VydEVucm9s
bC9DQSUyMHRlc3QlMjBzZXJ2ZXIuY3JsMDqgOKA2hjRmaWxlOi8vXFx6ai1yb3V0
ZXJcQ2VydEVucm9sbFxDQSUyMHRlc3QlMjBzZXJ2ZXIuY3JsMIGsBggrBgEFBQcB
AQSBnzCBnDBLBggrBgEFBQcwAoY/aHR0cDovL3pqLXJvdXRlci9DZXJ0RW5yb2xs
L3pqLXJvdXRlcl9DQSUyMHRlc3QlMjBzZXJ2ZXIoMSkuY3J0ME0GCCsGAQUFBzAC
hkFmaWxlOi8vXFx6ai1yb3V0ZXJcQ2VydEVucm9sbFx6ai1yb3V0ZXJfQ0ElMjB0
ZXN0JTIwc2VydmVyKDEpLmNydDANBgkqhkiG9w0BAQUFAANBABSEeYlEi7fm06en
NDdkZMjYV8LZB1JjniePwy1sUEEDa2bH9ZrcpTnJ+CSkCkxXBTc5ZWZnFTiSH/Oc
uVyQ9D8=
-----END CERTIFICATE-----
quit
% Certificate successfully imported
Ruijie(config)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

crypto pki sm2-identity

Supported by state code authentication, SM2 need an extra ID domain. If there is no special needs, the content of its ID will be “1234567812345678”. Refer to *SM2 Cryptography Algorithm Application Specification 0009-2012.*

crypto pki sm2-identity *string*

no crypto pki sm2-identity *string*

Parameter Description	Parameter	Description
	String	By default, ID used by SM2 is “1234567812345678”

Defaults N/A

Command Mode Global configuration mode

Usage Guide Default parameter. No command restores the default value.

Configuration Examples N/A

Related Commands

Command	Description
crypto pki import *ca_name* **pem terminal** *password* [**id** *string*]	Import certification and key from file with PEM （Privacy-enhanced Mail）format.

Platform Description N/A

crypto pki trustpoint

Use this command to enter trust point configuration mode (ca-trust point) in global configuration mode.
Use the **no** form of this command to delete the trust point and all its certificates.
crypto pki trustpoint *ca_name*
no crypto pki trustpoint *ca_name*

Parameter Description

Parameter	Description
ca_name	Common name of the CA corresponding to a trust point

Defaults N/A

Command Mode Global configuration mode

Usage Guide You can use this command to enter trust point configuration mode. In this mode, you can set all parameters corresponding to this trust point. If you run the **no crypto pki trustpoint ca_name** command, the trust point and all its associated certificates will deleted.

Configuration Examples N/A

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

debug crypto pki

Use this command to enable PKI debugging. Use the no form of this command to disable PKI debugging.

debug crypto pki { **event** | **error** }

no debug crypto pki { **event** | **error** }

Parameter Description	Parameter	Description
	event	PKI event debugging
	error	PKI error debugging

Defaults PKI debugging is disabled by default.

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

enrollment offline subject

Use this command to configure a distinguishable name for the local router in trustpoint configuration mode.

enrollment offline subject

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The distinguishable name is empty by default.

Command Mode Trust point configuration mode

Usage Guide You can use this command to fill in DN information when applying for a certificate. Type in the corresponding information based the prompt message.

```
Common Name (eg, YOUR name) []:         //Your first name and last name
Organizational Unit Name (eg, section) []:     //Name of your organizational
unit
Organization Name (eg, company) []:         //Name of your organization
Locality Name (eg, city) []:                  //Name of your city or district
State or Province Name (full name) []:         //Name of your state or province
Country Name (2 letter code) [CN]:             //2-letter country code
```

The preceding information is displayed in DN when the **show run** command is executed

Configuration Examples N/A

Related Commands	Command	Description
	crypto pki trustpoint	Enters trust point configuration mode.

Platform Description N/A

enrollment retry count

Use this command to specify the number of retries when SCEP is used to acquire the router certificate in trust point configuration mode.

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

enrollment retry count *number*

no enrollment retry count

Parameter Description	Parameter	Description
	number	A numeric value. The default value is 60 times.

Defaults The number of retries is 60 times by default.

Command Mode Trust point configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
crypto pki trustpoint	Enters trust point configuration mode.

Platform Description N/A

enrollment retry period

Use this command to specify the interval between request retries when SCEP is used to acquire the router certificate in trust point configuration mode.
Use the **no** form of this command to restore the default setting.
enrollment retry period *number*
no enrollment retry period

Parameter Description

Parameter	Description
number	A numeric value. The default value is one time per minute.

Defaults The default interval between request retries is one minute.

Command Mode Trust point configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
crypto pki trustpoint	Enters trust point configuration mode.

Platform Description N/A

enrollment url

Use this command to specify the URL to be used when SCEP is used to acquire the router certificate in trust point configuration mode.
Use the **no** form of this command to delete this URL.
enrollment url *url_string*
no enrollment url

Parameter Description

Parameter	Description
url_string	URL character string starting with http://, with length not exceeding 255

Defaults N/A

Command Mode Trust point configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
crypto pki trustpoint	Enters trust point configuration mode.

Platform Description N/A

enrollment auto-enroll

Ues this command to specify the update period of the certificate corresponding to the trust point in trust point configuration mode.
Use the **no** form of this command to restore the default setting.
enrollment auto-enroll *percentage*
no enrollment auto-enroll

Parameter Description

Parameter	Description
percentage	Ranges from 1 to 100 and specifies when the certificate will be updated.

Defaults N/A

Command Mode Trust point configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
crypto pki trustpoint	Enters trust point configuration mode.

Platform Description N/A

enrollment renewable

Use this command to enable the CA server corresponding to the trustpoint to support certificate update in trust point configuration mode.
Use the **no** form of this command to delete this URL.
enrollment renewable
no enrollment renewable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Trust point configuration mode.

Usage Guide N/A

Configuration Examples N/A

Related Commands	Command	Description
	crypto pki trustpoint	Enters trust point configuration mode.

Platform Description N/A

interface

Use this command to configure the source interface used by the trust point for certificate and CRL acquisition in trust point configuration mode.
Use the **no** form of this command to restore the default setting.
interface *interface_name*
no interface

Parameter Description	Parameter	Description
	none	Disables certificate validity check.

Defaults No source interface is configured by default.

Command Mode Trust point configuration mode

Usage Guide After the source interface is configured, the primary IP address of the source interface is used as the source address for certificate and CRL acquisition.

Configuration Examples N/A

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

recursion-check

Use this command to disable self-signature check of CA root certificates in trust point configuration mode.

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

recursion-check { **none** }
no recursion-check { **none** }

Parameter Description

Parameter	Description
none	Disables CA root certificate check.

Defaults The strict policy is used by default. That is, CA certificates must be self-signed certificates.

Command Mode Trust point configuration mode

Usage Guide The requirement that CA certificates be self-signed certificates is an approach for checking CA certificates during CA authentication. If CA certificates are not root certificates, higher-level certificates must be located recursively and used to verify the currently used CA certificate. In fact, if the certificate is issued by the same CA, it is trusted by the third party. In this case, the result is not affected by whether the CA certificate is a self-signed certificate. After recursion check is disabled, any certificate issued by the same CA can pass the authentication.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

revocation-check

Use this command to change the policy for verifying whether a certificate has been revoked in trust point configuration mode.
Use the **no** form of this command to restore the default setting.
revocation-check { **none** }
no revocation-check { **none** }

Parameter Description

Parameter	Description
none	Loose policy will be used during certificate verification. That is, the system does not verify whether a certificate has been revoked.

Defaults The strict policy is used by default. That is, CRL must be checked.

Command Mode Trust point configuration mode

Usage Guide When RGOS verifies the validity of the certificate owned by the communication peer, the verification of whether the certificate is revoked is implemented in strict mode and loose mode. In case of strict mode, the certificate must be verified for revocation. If the correct CRL is not found, the peer certificate will not be accepted. In case of loose mode, the certificate is not verified for revocation.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

asymmetric

Specify certificate algorithm. Use RSA algorithm in a default condition, and use SM2 algorithm in a specified condition.

asymmetric sm2

no asymmetric sm2

Parameter Description

Parameter	Description
sm2	Use SM2 for specified certificate algorithm.

Defaults Use RSA algorithm in a default condition

Command Mode Trust point configuration mode

Usage Guide Only the public and private key pair of online application or offline application mode certificate is generated locally. The specified algorithm will only take effect when generating key pairs. If import certificate directly, the command will not take any effect.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

time-check

Use this command to disable certificate validity check in trust point configuration mode.
Use the **no** form of this command to restore the default setting.
time-check { **none** }
no time-check { **none** }

Parameter Description

Parameter	Description
none	Disables certificate validity check.

Defaults Validity check is enabled by default. Expired certificates exceeding the validity range will fail the authentication during use.

Command Mode Trust point configuration mode

Usage Guide Certificate validity indicates whether certificates are valid. When used on equipment, certificates will be checked based on the system time. In certain extreme cases, the abnormal system time will result in failed certificate validity check, and this feature should be disabled to meet certain special applications. Since certificate check is bidirectional, as long as one side is configured not to check the validity, the same effect can be achieved. Use cautiously on the convergence side.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show crypto pki certificates

Use this command to query the certificate information configured by the system in privileged EXEC mode.

show crypto pki certificates [*CA_name*] [**detail**]

Parameter Description

Parameter	Description
CA_name	Trust point name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows the output of this command.

```
Ruijie# show crypto pki certificates test detail
%CA certificate info:                      //CA certificate information
Certificate:
Data:
Version: 3 (0x2)                          //X.509 v3 version
Serial Number:                                    //Serial number of the
certificate
7f:ff:bb:39:97:39:b4:81:4b:e1:6b:4f:f9:06:7a:4b
Signature Algorithm: sha1WithRSAEncryption   //Signature algorithm
Issuer: emailAddress=wlcpyjwb@star-net.cn, C=CN, ST=fj, L=fuzhou, O=Red
Giant, OU=Department 5, CN=CA Server
          //DN name of the issuer
Validity                                  //Certificate validity period
Not Before: Jun 22 05:46:32 2005 GMT    //Time of effectiveness in UTC
Not After : Jun 22 05:54:45 2007 GMT   //Time of expiration in UTC
Subject: emailAddress=wlcpyjwb@star-net.cn, C=CN, ST=fj, L=fuzhou, O=Red
Giant, OU=Department 5, CN=CA Server                                    //DN
name of the certificate subject
Subject Public Key Info:                   //Subject public key information
Public Key Algorithm: rsaEncryption          //Public key algorithm: RSA
encryption
RSA Public Key: (512 bit)             //512-bit RSA public key
Modulus (512 bit):
00:be:d1:e8:14:27:7a:30:2b:5e:11:ca:43:fd:2f:
2b:7e:a9:8a:07:96:a2:cf:fe:9d:b7:d3:da:54:c3:
03:4a:a8:44:b3:f0:11:dc:8a:bb:72:53:97:58:b1:
3f:df:6b:8a:9e:5f:46:d3:00:40:2e:24:d3:85:a7:
41:42:55:f7:75
Exponent: 65537 (0x10001)
```

```
X509v3 extensions:                          //Certificate extension information
X509v3 Key Usage:                             //Key usage identifier
Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
//Including digital signature, no repudiation, certificate signature, and CRL signature
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Subject Key Identifier:                  //Subject key identifier
64:46:12:C0:27:A4:9E:01:0C:65:DA:F8:6E:E7:FE:C6:56:EC:AD:D4
X509v3 CRL Distribution Points:          //CRL distribution point information
URI:http://zj-router/CertEnroll/CA%20Server.crl
URI:file://\\zj-router\CertEnroll\CA%20Server.crl
1.3.6.1.4.1.311.21.1:
...
Signature Algorithm: sha1WithRSAEncryption
 //Signature algorithm
34:2f:8d:93:68:43:60:7b:68:5f:f0:7e:91:0c:5c:e3:58:98:
7c:53:95:ae:c2:b8:1c:ff:82:a4:ae:95:a8:81:a8:8a:ff:f9:
6f:92:72:3e:fa:6f:84:7d:83:47:93:0f:85:76:48:ae:68:b9:
5a:72:cf:09:50:be:1b:a7:e1:87                //Certificate signature
%Router certificate info:           //Router certificate information:
Certificate:
Data:
Version: 3 (0x2)                            //X.509 v3 version
Serial Number:                                    //Serial number of the
certificate
16:2a:7a:1d:00:00:00:00:00:02
Signature Algorithm: sha1WithRSAEncryption
 //Signature algorithm
Issuer: emailAddress=wlcpyjwb@star-net.cn, C=CN, ST=fj, L=fuzhou, O=Red
Giant, OU=Department 5, CN=CA Server
//DN name of the issuer
Validity                                   //Certificate validity period
Not Before: Jun 22 05:50:48 2005 GMT       //Time of effectiveness in UTC
Not After : Jun 22 06:00:48 2006 GMT       //Time of expiration in UTC
Subject: emailAddress=zhaojun, C=CN, ST=fj, L=fuzhou, O=Red Giant, OU=De
partment 5, CN=zhaojun
//DN name of the certificate subject
Subject Public Key Info:                    //Subject public key information
Public Key Algorithm: rsaEncryption           //Public key algorithm: RSA
encryption
RSA Public Key: (2048 bit)           //2048-bit RSA public key
Modulus (2048 bit):
00:c6:e2:7a:e8:8d:6d:d8:bb:56:a8:9c:03:62:14:
e5:2e:23:e5:a5:26:31:3d:b2:24:65:b1:f2:cc:07:
e3:ef:cc:02:3c:d0:6e:00:8d:fc:ce:3a:b6:45:7a:
```

```
cb:a0:87:94:1f:c3:92:43:36:6a:b2:7c:9c:d5:ca:
7e:83:ba:76:49:7f:be:f4:1f:4a:a1:0b:98:22:96:
e2:79:54:a0:ed:1c:62:30:b7:ee:6a:6e:cb:72:e9:
9c:d9:e8:b0:dc:f5:c6:19:8f:2b:2a:85:fa:bf:ff:
08:40:7e:f2:a1:df:d1:8b:ef:68:32:1e:1a:45:fa:
16:de:33:b0:62:90:bd:9c:8e:ec:7c:6e:49:48:75:
e6:5c:ce:b1:8e:1c:80:f3:5b:79:6c:a1:31:b2:a9:
48:37:9f:ed:45:95:85:ba:98:0f:42:c5:78:4c:3d:
a2:45:73:90:3d:0b:1a:7c:53:b5:97:1a:a6:43:2f:
44:54:0f:a1:51:3a:0e:9f:8b:2e:d1:70:cb:36:99:
91:57:d2:b7:9d:7c:ee:07:cf:4a:c7:cd:71:dc:ce:
72:dc:75:a0:03:b2:36:be:8e:af:ca:99:46:03:83:
27:d3:ff:24:1e:4c:0c:21:99:b4:fe:5a:4d:61:b5:
e9:b4:38:dc:59:2c:37:f3:93:02:fc:09:88:02:1b:
d0:45
Exponent: 65537 (0x10001)
X509v3 extensions:                          //Certificate extension information
X509v3 Key Usage: critical     //Key usage identifier, which is the key extension
Digital Signature, Non Repudiation   //Including digital signature and non
repudiation
X509v3 Extended Key Usage:                  //Extended key usage
1.3.6.1.5.5.8.2.2
X509v3 Subject Key Identifier:                   //Subject key identifier
84:7E:33:A3:91:A5:26:1D:2D:BB:54:65:BF:C7:2A:2A:2E:87:D5:A9
X509v3 Authority Key Identifier:       //Key identifier of the issuance
organization
keyid:64:46:12:C0:27:A4:9E:01:0C:65:DA:F8:6E:E7:FE:C6:56:EC:AD:D4
DirName:/emailAddress=wlcpyjwb@star-net.cn/C=CN/ST=fj/L=fuzhou/O
=Red Giant/OU=Department 5/CN=CA Server
serial:7F:FF:BB:39:97:39:B4:81:4B:E1:6B:4F:F9:06:7A:4B
X509v3 CRL Distribution Points:         //CRL distribution point information
URI:http://zj-router/CertEnroll/CA%20Server.crl
URI:file://\\zj-router\CertEnroll\CA%20Server.crl
Authority Information Access:           //Information access point of the
issuance organization
CA Issuers - URI:http://zj-router/CertEnroll/zj-router_CA%20Serv
er.crt
CA Issuers - URI:file://\\zj-router\CertEnroll\zj-router_CA%20Se
rver.crt
Signature Algorithm: sha1WithRSAEncryption   //Signature algorithm
37:50:0c:d6:6c:23:6d:2d:81:37:02:6c:22:ef:e2:95:98:dc:
91:25:fe:0a:3b:b0:f2:48:69:2c:6b:98:66:be:6b:09:ef:de:
2f:db:ed:71:0e:04:a5:12:38:8b:30:2b:eb:c9:d9:88:1e:a2:
10:2c:86:d2:3d:25:fd:9c:df:b4/               //Certificate signature
Ruijie#
```

Related Commands	Command	Description
	N/A	N/A

Note Log service statistics are displayed.

Platform Description N/A

show crypto pki crls

Use this command to query the CRL information of the system in privileged EXEC mode.

show crypto pki crls [*CA_name*] [**detail**]

Parameter Description	Parameter	Description
	CA_name	Trust point name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the output of this command.

```
Ruijie# sh crypto pki crls test detail
Certificate Revocation List (CRL):
Version 2 (0x1)                     //CRL version of X.509V2
Signature Algorithm: sha1WithRSAEncryption    //Signature algorithm
Issuer:       /emailAddress=wlcpyjwb@star-net.cn/C=CN/ST=fj/L=fuzhou/O=Red
Giant/OU=Department 5/CN=CA Server
                   //DN of the issuer
Last Update: Jun 22 06:10:27 2005 GMT  //Time of last update in UTC
Next Update: Jun 29 18:30:27 2005 GMT  //Time of next update in UTC, namely
the expiration time of CRL
CRL extensions:                    //CRL extensions:
X509v3 Authority Key Identifier:       //Key identifier of the issuance
organization
```

```
keyid:64:46:12:C0:27:A4:9E:01:0C:65:DA:F8:6E:E7:FE:C6:56:EC:AD:D4
1.3.6.1.4.1.311.21.1:...
Revoked Certificates:                //List of revoked certificates:
Serial Number: 162A7A1D000000000002        //Serial number of the revoked
certificate
Revocation Date: Jun 22 06:19:53 2005 GMT    //Revocation time
CRL entry extensions:                    //CRL entry extensions
X509v3 CRL Reason Code:                //CRL revocation cause code
Key Compromise                                //Key compromise
Serial Number: 1635E5E3000000000003
Revocation Date: Jun 22 06:19:53 2005 GMT
CRL entry extensions:
X509v3 CRL Reason Code:
Key Compromise                                //Key compromise
Signature  Algorithm:  sha1WithRSAEncryption        //Signature  algorithm
5d:a2:ab:07:ff:7e:0e:9a:af:b2:25:11:7f:31:86:aa:21:48:
37:e7:22:99:e3:b2:15:e0:f9:80:63:66:5e:2f:f2:d6:c0:ea:
ef:46:7e:d1:c1:b2:66:0e:0b:d3:74:d1:55:bc:5c:13:46:e8:
56:ec:40:83:7b:1b:75:f2:68:87                 //Signature value
Ruijie#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show crypto pki trustpoints

Use this command to query the trust point configuration of the system in privileged EXEC mode.

show crypto pki trustpoints

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 this command.

```
Ruijie(config)#show crypto pki trustpoints
Trustpoint CA
  enrollment url http://192.168.50.203/certsrv/mscep/mscep.dll
  enrollment retry perriod 1
  enrollment retry count 60

Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show crypto pki trustpoints *name_string* status

Use this command to query the current state of the trustppoint of the system in privileged EXEC mode.

show crypto pki trustpoints *name_string* **status**

Parameter Description

Parameter	Description
name_string	Name of the trust point

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the output of this command.

```
Ruijie(config)#show crypto pki trustpoints CA status
Trustpoint CA Status:
  State:
    Keys generated ..... Not Generated
    Issuing CA authenticated ....... No
    Certificate request(s) ..... No
```

```
Ruijie(config)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

VPDN Commands

vpdn authorize

Use this command to enable VPDN authentication.
Use the **no** form of this command to disable VPDN authentication.
vpdn authorize domain [**split**]
no vpdn authorize domain [**split**]

Parameter Description

Parameter	Description
domain	Domain authentication switch
split	Domain split switch

Defaults Domain authentication is disabled by default.

Command Mode Global configuration mode

Usage Guide This command can be executed only after the **vpdn enable** command is executed.
Domain authentication refers to local domain authentication.
After the **split** option is configured, domain information in the username will be split after domain resolution, leaving only the username to be transferred to the authentication module.

Configuration Examples The following example enables the VPDN domain name resolution function.

```
Ruijie(config)# vpdn authorize domain split
Ruijie(config)#
```

Related Commands

Command	Description
vpdn domain-delimiter	Configures domain name resolution.
domain	Configures the domain name.

Platform Description N/A

vpdn domain-delimiter

Use this command to configure VPDN domain name resolution.
Use the **no** form of this command to remove VPDN domain name resolution.
vpdn domain-delimiter *LINE* [**prefix | suffix**]
no vpdn domain-delimiter

Parameter Description

Parameter	Description
LINE	Domain name identification delimiter. Only @, /, %, #, - , and \ can be identified. With \ enabled, \\ can also be identified.
prefix	(Optional) prefix
suffix	(Optional and default) suffix

Defaults VPDN domain name resolution is disabled by default.

Command Mode Global configuration mode

Usage Guide The domain name is resolved from the user name according to the wildcards, prefix, and suffix.
You can run this command only after the **vpdn enable** command is configured.
The prefix and suffix are optional, and the suffix is the default configuration.
The delimiter can only identify any of @, /, %, #, -, and \\. You can configure all characters as the prefix delimiter or suffix delimiter, but the prefix delimiter must not conflict with the suffix delimite. That is, a character cannot be the prefix delimiter and suffix delimiter at the same time.
If there are multiple delimiters in a user name, the prefix matches the first delimiter and the suffix matches the last one based on configuration. For example:
aaa@a@#a%a
If @ is prefix delimiter and % is the suffix delimiter, the domain name matched by prefix is aaa, while the domain name matched by suffix is a. As the suffix is preferred, the obtained domain name is a.
If # is prefix delimiter and @ is the suffix delimiter, then the prefix is aaa@a@ and the suffix is #a%a.

Configuration Examples The following example enables VPDN domain name resolution.

```
Ruijie(config)# vpdn domain-delimiter @/%#-\
Ruijie(config)#
```

Related Commands

Command	Description
vpdn authorize	Configures domain name split.
domain	Configures the domain name.

Platform Description N/A

vpdn enable

Use this command to enable the VPDN function.
Use the **no** form of this command to disable the VPDN function.
vpdn enable
no vpdn enable

Defaults The VPDN function is disabled by default.

Command Mode Global configuration mode

Usage Guide Except the client-initiated L2TP tunnel that does not require the system to enable the VPDN function, RGOS requires the system to enable the VPDN function no matter whether it provides the LAC or LNS function, or whether it uses the PPTP or L2TP protocol. Effective setting or change of this command will immediately cause the relevant existing tunnels to be removed actively and forcibly.

Configuration Examples The following example enables the VPDN function.

```
Ruijie(config)# vpdn enable
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn ignore source

Use this command to enable the VPDN source address ignoring function. After this command is executed, the source addresses of the data packets received will not be checked.
Use the **no** form of this command to strictly check the source addresses of the packets sent from the peer end.
vpdn ignore source
no vpdn ignore source

Parameter Description

Parameter	Description
N/A	N/A

Defaults The system checks the source addresses of tunnel packets by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the VPDN source address ignoring function, which takes effect only for express forwarding data.

Configuration Examples The following example enables the VPDN source address ignoring function.

```
Ruijie(config)# vpdn ignore_source
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn limit rate

Use this command to set the number of VPDN tunnels allowed to be created at one time in order to limit the rate of creating VPDN.
Use the **no** formof this command to restore the default setting.
vpdn limit_rate *rate_num*
no vpdn limit_rate

Parameter Description

Parameter	Description
rate_num	Number of VPDN tunnels allowed to be created at one time, ranging from 5 to 100

Defaults The rate of creating VPDN tunnels is not limited by default.

Command Mode Global configuration mode

Usage Guide When there are too many VPDN dial-ins, system performance is affected. This command can be used to limit the dial-in number.

Configuration Examples The following example sets the number of negotiated tunnels that are allowed at one time to 50.

```
Ruijie(config)# vpdn limit_rate 50
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn send limit_rate

Use this command to limit the number of ICRQ packets that can be sent at a time. Use the **no** form of this command to restore the default setting.

vpdn send limit_rate *rate_num*
no vpdn send limit_rate

Parameter Description

Parameter	Description
rate_num	Indicates the number of ICRQ packets sent at a time. The value range is from **5** to **100**.

Defaults No rate limit is configured by default.

Command Mode Global configuration mode

Usage Guide When there are too many sessions initiated by the LAC, system performance is affected. This command can be used to limit the ICRQ rate.

Configuration Examples The following example sets the ICRQ rate limit to 100.

```
Ruijie(config)# vpdn send limit_rate 50
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn session-limit

Use this command to set the maximum number of sessions allowed when the system provides the VPDN function.
Use the **no** form of this command to restore the default setting.
vpdn session-limit *sessions*
no vpdn session-limit

Parameter Description

Parameter	Description
sessions	Maximum number of sessions allowed when the system provides the VPDN function

Defaults By default, this value is set to the maximum number of sessions that the system can provide. For the 36 series, the value is 300.

Command Mode Global configuration mode

Usage Guide When there are too many VPDN dial-ins, system performance is affected.. This command can be used to limit the number of dial-ins.

Configuration Examples The following example sets the maximum number of sessions currently accepted to 100.

```
Ruijie(config)# vpdn session-limit 100
Ruijie(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn source-ip

Use this command to set the local (source) address that the system uses when providing the VPDN function.
Use the **no** form to restore the default setting.
vpdn source-ip *A.B.C.D*
no vpdn source-ip

Parameter Description

Parameter	Description
A.B.C.D	Local address that the system uses when providing the VPDN function

Defaults By default, the system has no local (source) address that is set to provide the VPDN function.

Command Mode Global configuration mode

Usage Guide If the system provides the LNS (L2TP) or HGW (PPTP) function, this command can be used to limit the destination addresses of all the currently accepted tunnel connection requests to the specified address. Effective setting or change of this command will immediately cause the relevant existing tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the destination addresses of all the currently accepted tunnel connection requests to 192.168.12.223.

```
Ruijie(config)# vpdn source-ip 192.168.12.223
Ruijie(config)#
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

clear vpdn tunnel

Use this command to forcibly clear the specified tunnel.

clear vpdn tunnel [{ **l2tp** | **pptp** } [*remote-host-name*]]

Parameter Description

Parameter	Description
l2tp	L2TP tunnel
pptp	PPTP tunnel
remote-host-name	Name of the remote host of the tunnel

Platform Description N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to forcibly clear the specified tunnel. If no parameter is used, all the existing tunnels (including PPTP and L2TP tunnels) will be cleared forcibly. If only the tunneling protocol is specified, all the tunnels corresponding to the tunneling protocol will be cleared forcibly. If the name of the remote host of the tunnel is also specified, the tunnel with the name that matches the remote host name of the tunnel among the tunnels that correspond to the tunneling protocol will be cleared forcibly.

Configuration Examples The following example clears all the existing L2TP tunnels.

```
Ruijie# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
1    1    BLIZZARD   est    192.168.12.213  1701  1  1
LocID     RemID     TunID     Username, Intf/
State  Last Chg                    Vcid, Circuit
1         1         1         ms,Vi1             est
00:46:30
%No active PPTP tunnels
Ruijie# clear vpdn tunnel l2tp
Ruijie#
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
```

```
%CHANGED: Interface Virtual-Access1, changed state to administratively down
Ruijie# show vpdn
%No active L2TP tunnels
%No active PPTP tunnels
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug vpdn

Use this command to turn on or off the output of VPDN debugging information.

debug vpdn [**error** | **event** | **l2x-data** | **l2x-errors** | **l2x-events** | **l2x-packets** | **packet**]

no debug vpdn [**error** | **event** | **l2x-data** | **l2x-errors** | **l2x-events** | **l2x-packets** | **packet**]

Parameter Description

Parameter	Description
error	VPDN protocol error report
event	VPDN protocol negotiation process event
l2x-data	L2TP data sending
l2x-errors	L2TP protocol error report
l2x-events	L2TP protocol negotiation process event
l2x-packets	Resolution of content in the L2TP protocol control packet
packet	Resolution of content in the VPDN protocol packet

Defaults N/A

Command Mode Common user mode and privileged EXEC mode

Usage Guide When debugging networks and diagnosing network faults, users can use this command to track establishment of VPDN tunnels and sessions, and events, errors, and detailed control packet information during operation. The **error**, **event**, and **packet** parameters are common to the VPDN protocols (L2TP and PPTP), while other parameters are valid only for the L2TP protocol.

Configuration Examples The following example shows the output of the **debug vpdn event** command during creation of PPTP tunnels and sessions.

```
VPDN: Pptp recv start-control-connection-request from host 192.168.200.114
PPTP: New tunnel socket id =9
VPDN: Pptp get tunnel info for 192.168.200.114 ok!
VPDN: Pptp send start-control-connection-reply, ok
```

```
VPDN: Pptp tunnel id 0 state change: idle --> estbed
PPTP: Add send-echo-request timer, interval = 60
VPDN: Pptp tunnel id 0 recv outgoing-call-request!
Pptp: Tunnel to 192.168.200.114 get config para. from vpdn-group pptp!
VPDN: Must process using ACCEPT_DIALIN parameters
Pptp: Session va0 get config para. from vpdn-group pptp!
VPDN: Pptp session va0 state change: idle --> connected
PPTP: Receive outcall request,process ok!assign local call id = 1
VPDN: Pptp tunnel id 0 send out-call reply
%LINK CHANGED: Interface virtual-access 0, changed state to up
VPDN: Pptp tunnel to 192.168.200.114 peer callid 1 recv set-linkinfo
VPDN: Pptp tunnel to 192.168.200.114 peer callid 1 recv set-linkinfo
%LINE PROTOCOL CHANGE: Interface virtual-access 0, changed state to UP
```

The following example shows the output of the **debug vpdn packet** command during creation of PPTP tunnels and sessions.

```
PPTP: I Start-Control-Connection-Request len 156 Magic Cookie 0x1A2B3C4D
Protocol Version 0x100
Framing Type 0x1
Bearer Type 0x1
Maximum Channels 0x0
Firmware Revision 0x893
Host Name:
endor String: Microsoft Windows NT
PPTP: O Start-Control-Connection-Reply len 156 Magic Cookie 0x1A2B3C4D
Protocol Version 0x100
Framing Type 0x2
Bearer Type 0x3
Maximum Channels 0x0
Firmware Revision 0x100
Host Name: Dingjs
Vendor String: Ret-Giant Network Operating System
PPTP: I Outgoing-Call-Request len 168 Magic Cookie 0x1A2B3C4D
Call Id 0x4000
Call Serial Number 0x96A5
Min BPS 0x12C
Max BPS 0x5F5E100
Bearer Type 0x3
Framing Type 0x3
Rec Window Size 0x40
Proc Delay 0x0
Phone Number Length 0x0
Phone Number:
Subaddress:
PPTP: O Outgoing-Call-Reply len 32 Magic Cookie 0x1A2B3C4D
```

```
Call Id 0x1
Peer Call Id 0x4000
Result Code 0x1
Error Code 0x0
Cause Code 0x0
Connect Speed 0xFA00
Rec Window Size 0x10
Physical Channel Id 0x0
PPTP: I Set-Link-Info len 24 Magic Cookie 0x1A2B3C4D
Peer Call Id 0x1
Send ACCM 0xFFFFFFFF
Recv ACCM 0xFFFFFFFF
%UPDOWN: Interface Virtual-Access1, changed state to up
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 64 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
PPTP: I Set-Link-Info len 24 Magic Cookie 0x1A2B3C4D
Peer Call Id 0x1
Send ACCM 0xFFFFFFFF
Recv ACCM 0xFFFFFFFF
Vi1 VPDN PROCESS Into tunnel: Sending 45 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 46 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 187 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 56 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 64 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
Vi1 VPDN PROCESS Into tunnel: Sending 52 byte pak
```

The following example shows the output of the **debug vpdn error** command when the physical connection of a PPTP tunnel is disconnected.

```
VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=37, ack=36),
decrease send window to half of current = 33!
VPDN: PPTP session Virtual-Access1 adjust ATO to 220 ms!
VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=38, ack=36),
decrease send window to half of current = 16!
VPDN: PPTP session Virtual-Access1 adjust ATO to 280 ms!
VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=39, ack=36),
decrease send window to half of current = 8!
VPDN: PPTP session Virtual-Access1 adjust ATO to 400 ms!
VPDN: Pptp EGRE encap fail, err=-4!
VPDN: PPTP session Virtual-Access1 wait pak ack timeout(wait seq=40, ack=36),
decrease send window to half of current = 4!
VPDN: PPTP session Virtual-Access1 adjust ATO to 640 ms!
```

The following example shows the overall VPDN debugging during the process in which LNS accepts

the dial-in request from the peer end and finally establishes a tunnel (including the channel and session).

```
Ruijie# debug vpdn error
vpdn protocol errors debugging is on
Ruijie# debug vpdn event
vpdn events debugging is on
Ruijie# debug vpdn packet
vpdn packet debugging is on
Ruijie# show debug
VPDN:
vpdn events debugging is on
vpdn protocol errors debugging is on
vpdn packet debugging is on
Ruijie#
VPDN PROCESS From tunnel: Received 158 byte pak
L2X: UDP socket write 168 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 70 byte pak
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 76 byte pak
Get virtual-access from free queue: Virtual-Access1
Clone virtual-access from interface Virtual-Template1
L2X: UDP socket write 56 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 76 byte pak
L2X: UDP socket write 40 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
Vi1 Tnl/Sn 3/1 L2TP: Virtual interface created for unknown, bandwidth 1024
Kbps
Vi1 Tnl/Sn 3/1 L2TP: VPDN session up
VPDN PROCESS From tunnel: Pak consumed
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
%UPDOWN: Interface Virtual-Access1, changed state to up
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
L2X: UDP socket write 54 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
```

```
L2X: UDP socket write 54 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
L2X: UDP socket write 54 bytes, 255.255.255.255(1701) to 4.83.68.68(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 54 byte pak
L2X: UDP socket write 54 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Received 54 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 18 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
VPDN PROCESS From tunnel: Received 56 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 20 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 45 byte pak
L2X: UDP socket write 45 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
VPDN PROCESS From tunnel: Received 50 byte pak
Vi1 VPDN PROCESS From tunnel: Queue 14 byte pak to ppp parse and iqueue
Vi1 VPDN PROCESS From tunnel: Pak send successful
Vi1 VPDN PROCESS Into tunnel: Sending 50 byte pak
L2X: UDP socket write 50 bytes, 192.168.12.217(1701) to 192.168.12.242(1701)
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

The following example shows the **debug vpdn l2x-data** debugging during the process in which LNS accepts the dial-in request and finally establishes a tunnel (including the channel and session).

```
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
```

```
L2X: Punting to L2TP control message queue
L2X: Punting to L2TP control message queue
%UPDOWN: Interface Virtual-Access1, changed state to up
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

The following example shows the **debug vpdn l2x-error** output when authentication of L2TP tunnels fails.

```
Tnl 14 L2TP: Tunnel auth failed for BLIZZARD
Tnl 14 L2TP: Expected
9E 8D 7A 8E 78 EA 41 9F A1 74 01 21 DE 4F F3 F0
Tnl 14 L2TP: Got
84 E5 62 69 AE 46 A5 98 4E FE E2 38 EE F2 B7 E2
```

The following example shows the **debug vpdn l2x-events** debugging during the process in which LNS accepts the dial-in request from the peer end and finally establishes a tunnel (including the channel and session).

```
L2TP: I SCCRQ from C3640 tnl 26656
New tunnel created for remote C3640, address 192.168.12.242
Tnl 0 L2TP: Got a challenge in SCCRQ, C3640
Tnl 20 L2TP: O SCCRP  to C3640 tnlid 26656
Tnl 20 L2TP: Control channel retransmit delay set to 1 seconds
Tnl 20 L2TP: Tunnel state change from idle to wait-ctl-conn
Tnl 20 L2TP: I SCCCN from C3640 tnl 26656
Tnl 20 L2TP: Got a Challenge Response in SCCCN, C3640
Tnl 20 L2TP: Tunnel Authentication success
Tnl 20 L2TP: Tunnel state change from wait-ctl-conn to established
Tnl 20 L2TP: SM State established
Tnl 20 L2TP: I ICRQ from C3640 tnl 26656
Tnl/Sn 20/1 L2TP: Accepted ICRQ, new session created
Tnl/Sn 20/1 L2TP: O ICRP to C3640 26656/1279
Tnl/Sn 20/1 L2TP: Session state change from idle to wait-connect
Tnl 20 L2TP: Control channel retransmit delay set to 1 seconds
Tnl/Sn 20/1 L2TP: I ICCN from C3640 tnl 26656, cl 1279
Tnl/Sn 20/1 L2TP: Session state change from wait-connect to
wait-for-service-sel
ection-iccn
Vi1 Tnl/Sn 20/1 L2TP: Session state change from wait-for-service-selection-
iccn to established
%UPDOWN: Interface Virtual-Access1, changed state to up
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

The following example shows the **debug vpdn l2x-packets** debugging during the process in which LNS accepts the dial-in request from the peer end and finally establishes a tunnel (including the channel and session).

```
L2TP: I SCCRQ from C3640 tnl 18889
```

```
L2X: Parse  AVP 0, len 8, flag 0x8000 (M)
L2X: Parse SCCRQ
L2X: Parse  AVP 2, len 8, flag 0x8000 (M)
L2X: Protocol Ver 1
L2X: Parse  AVP 6, len 8, flag 0x0
L2X: Firmware Ver 0x1130
L2X: Parse  AVP 7, len 11, flag 0x8000 (M)
L2X: Hostname C3640
L2X: Parse  AVP 8, len 25, flag 0x0
L2X: Vendor Name Cisco Systems, Inc.
L2X: Parse  AVP 10, len 8, flag 0x8000 (M)
L2X: Rx Window Size 800
L2X: Parse  AVP 11, len 22, flag 0x8000 (M)
L2X: Chlng
       98 20 4E 34 6A 4C E1 E7 FA CF 58 07 FF 4E 56 A3
L2X: Parse  AVP 9, len 8, flag 0x8000 (M)
L2X: Assigned Tunnel ID 18889
L2X: Parse  AVP 3, len 10, flag 0x8000 (M)
L2X: Framing Cap 0x3
L2X: Parse  AVP 4, len 10, flag 0x8000 (M)
L2X: Bearer Cap 0x3
L2X: No missing AVPs in SCCRQ
L2X: I SCCRQ, flg TLS, ver 2, len 130, tnl 0, ns 0, nr 0 contiguous pak, size
130
C8 02 00 82 00 00 00 00 00 00 00 80 08 00 00
00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
00 06 11 30 80 0B 00 00 00 07 43 33 36 34 30 00
19 00 00 00 08 43 69 73 63 6F 20 53 79 73 74 65
6D 73 2C 20 49 6E 63 2E ...
Tnl 22 L2TP: O SCCRP  to C3640 tnlid 18889
Tnl 22 L2TP: O SCCRP, flg TLS, ver 2, len 140, tnl 18889, ns 0, nr 1
C8 02 00 8C 49 C9 00 00 00 00 00 01 80 08 00 00
00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
00 03 00 00 00 01 80 0A 00 00 00 04 00 00 00 00
00 08 00 00 00 06 11 30 80 0A 00 00 00 07 52 36
32 31 00 0E 00 00 00 08 ...
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 1, nr 1
C8 02 00 0C 49 C9 00 00 00 01 00 01
Tnl 22 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
Tnl 22 L2TP: Parse SCCCN
Tnl 22 L2TP: I SCCCN from C3640 tnl 18889
Tnl 22 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
Tnl 22 L2TP: Chlng Resp
5C D5 A4 37 36 A6 7D 0F FE EF 22 48 B8 DF F5 12
Tnl 22 L2TP: No missing AVPs in SCCCN
```

```
Tnl 22 L2TP: I SCCCN, flg TLS, ver 2, len 42, tnl 22, ns 1, nr 1 contiguous
pak, size 42
C8 02 00 2A 00 16 00 00 00 01 00 01 80 08 00 00
00 00 00 03 80 16 00 00 00 0D 5C D5 A4 37 36 A6
7D 0F FE EF 22 48 B8 DF F5 12
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 1, nr 2
C8 02 00 0C 49 C9 00 00 00 01 00 02
Tnl 22 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
Tnl 22 L2TP: Parse ICRQ
Tnl 22 L2TP: I ICRQ from C3640 tnl 18889
Tnl 22 L2TP: Parse  AVP 15, len 10, flag 0x8000 (M)
Tnl 22 L2TP: Serial Number -1714567290
Tnl 22 L2TP: Parse  AVP 14, len 8, flag 0x8000 (M)
Tnl 22 L2TP: Assigned Call ID 1280
Tnl 22 L2TP: Parse  AVP 18, len 10, flag 0x8000 (M)
Tnl 22 L2TP: Bearer Type 0
Tnl 22 L2TP: No missing AVPs in ICRQ
Tnl 22 L2TP: I ICRQ, flg TLS, ver 2, len 48, tnl 22, ns 2, nr 1 contiguous
pak,size 48
C8 02 00 30 00 16 00 00 00 02 00 01 80 08 00 00
00 00 00 0A 80 0A 00 00 00 0F 99 CD C7 86 80 08
00 00 00 0E 05 00 80 0A 00 00 00 12 00 00 00 00
Tnl/Sn 22/1 L2TP: O ICRP to C3640 18889/1280
Tnl/Sn 22/1 L2TP: O ICRP, flg TLS, ver 2, len 28, tnl 18889, lsid 1, rsid 1280,ns
1, nr 3
C8 02 00 1C 49 C9 05 00 00 01 00 03 80 08 00 00
00 00 00 0B 80 08 00 00 00 0E 00 01
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 2, nr 3
C8 02 00 0C 49 C9 00 00 00 02 00 03
Tnl/Sn 22/1 L2TP: I ICCN from C3640 tnl 18889, cl 1280
Tnl/Sn 22/1 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
Tnl/Sn 22/1 L2TP: Parse ICCN
Vi1 Tnl/Sn 22/1 L2TP: Parse  AVP 24, len 10, flag 0x8000 (M)
Vi1 Tnl/Sn 22/1 L2TP: Connect Speed 0
Vi1 Tnl/Sn 22/1 L2TP: Parse  AVP 19, len 10, flag 0x8000 (M)
Vi1 Tnl/Sn 22/1 L2TP: Framing Type 1
Tnl/Sn 22/1 L2TP: No missing AVPs in ICCN
Tnl/Sn 22/1 L2TP: I ICCN, flg TLS, ver 2, len 48, tnl 22, lsid 1, rsid 1280,
ns 3, nr 2 contiguous pak, size 48
C8 02 00 30 00 16 00 01 00 03 00 02 80 08 00 00
00 00 00 0C 80 0A 00 00 00 18 00 00 00 00 80 0A
00 00 00 13 00 00 00 01 00 08 00 00 00 1D 00 04
Tnl 22 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 18889, ns 2, nr 4
C8 02 00 0C 49 C9 00 00 00 02 00 04
%UPDOWN: Interface Virtual-Access1, changed state to up
```

```
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show vpdn

Use this command to query information about the VPDN tunnel specified in the current system.

show vpdn [**session | tunnel** [{ **l2tp** | **pptp** } *locid*]]

Parameter Description

Parameter	Description
session	Displays all the sessions.
tunnel	Displays all the tunnels.
l2tp *locid*	Displays details about the L2TP tunnel with the specified ID.
pptp *locid*	Displays details about the PPTP tunnel with the specified ID.

Defaults N/A

Command Mode Common user mode and privileged EXEC mode

Usage Guide You can run this command to view the VPDN tunnel information in the current system in real time. If no parameter is specified, all the VPDN tunnels and sessions in the current system will be displayed.
Note: As the length of the user name is not limited, for the purpose of display alignment, only the first 12 charaters of the user name are listed.
To view the complete user name, run the **show vpdn tunnel l2tp locid** and **show vpdn tunnel pptp locid** commands.

Configuration Examples Example 1: displays information about all the VPDN tunnels in the current system.

```
Ruijie# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
4     77    BLIZZARD     est    192.168.12.213  1701  1        1
LocID     RemID     TunID     Username, Intf/     State  Last Chg
                              Vcid, Circuit
1         1         4         ms,Vi1              est    00:33:58
%No active PPTP tunnels
```

```
Ruijie#
```

The following example displays information about all the VPDN channels in the current system.

```
Ruijie# show vpdn tunnel
L2TP Tunnel Information Total tunnels 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
4     77    BLIZZARD     est    192.168.12.213  1701  1        1
%No active PPTP tunnels
Ruijie#
```

The following example displays information about all the VPDN sessions in the current system.

```
Ruijie# show vpdn session
L2TP Session Information Total sessions 1
LocID     RemID     TunID     Username, Intf/     State  Last Chg
                             Vcid, Circuit
1         1         4         ms,Vi1              est    00:37:03
%No active PPTP tunnels
Ruijie#
```

Example 2: displays details about the specified PPTP or L2TP tunnel.

The following example displays details about the L2TP tunnel with the specified ID.

```
Ruijie# show vpdn tunnel l2tp 4
L2TP tunnel locid 4 is up,remote id is 77, 1 active sessions
  Tunnel state is est
  Tunnel transport is UDP
  Remote tunnel name is BLIZZARD
    Internet Address 192.168.12.213, port 1701
  Local tunnel name is LNStest
    Internet Address 192.168.12.212, port 1701
  VPDN group for tunnel is 1
  Tunnel domain unknown
  ip mtu adjust disabled
  Control Ns 2, Nr 4
```

The following example displays details about thePPTP tunnel with the specified ID.

```
Ruijie#show vpdn tunnel
%No active L2TP tunnels
PPTP Tunnel Information Total tunnels 1
LocID Remote Name    State      Remote Address  Port  Sessions
2                 estbed      192.168.45.160  3077  1
Ruijie#
Ruijie#show vpdn tunnel pptp 2
PPTP tunnel id 2 is up, remote id is 0, 1 active session
  Tunnel state is estbed
  Remote tunnel name is
    Internet Address 192.168.45.160, port 3077
  Local tunnel name is
    Internet Address 192.168.45.161
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

VPDN-Group Commands

accept dialin

Use this command to set the tunnel working mode to accept dial-in.
Use the **no** form of this command to restore the default setting.
accept-dialin
no accept-dialin

Parameter Description

Parameter	Description
N/A	N/A

Defaults The tunnel working mode is not set by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide The system does not specify any tunnel working mode for VPDN-Group by default. Users must first set the tunnel working mode before setting the tunnel working protocol and the bound virtual template interface. Effective setting or change of this command will immediately cause the relevant existing tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the tunnel working mode to accept dial-in.

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

dns

Use this command to set the address used by the PPP protocol for DNS negotiation during tunnel negotiation.
Use the **no** form of this command to restore the default setting.
dns *A.B.C.D A.B.C.D*
no dns

Parameter

Parameter	Description

Description	*A.B.C.D*	Address for DNS negotiation through PPP

Defaults No address is specified for DNS negotiation through PPP by default.

Command Mode VPDN-domain configuration mode

Usage Guide Use this command to set the address for DNS negotiation through PPP based on a domain name. When tunnel negotiation is successful, the DNS address is found based on the domain name. Then, the specified address is used for DNS negotiation.

Configuration Examples The following example specifies the address for DNS negotiation through PPP based on the domain name ruijie.

```
Ruijie(config-vpdn)# domain ruijie
Ruijie(config-vpdn-domain)# dns 1.1.1.1 2.2.2.2
Ruijie(config-vpdn-domain)#
```

Related Commands	Command	Description
	domain	Configures a domain name.

Platform Description N/A

domain

Use this command to set the domain field corresponding to the group.
domain *domain-name* [**vrf** *vrf-name*]
no domain *domain-name*

Parameter Description	Parameter	Description
	domain-name	Domain name
	vrf	Specify the type as VRF.
	vrf-name	VRF name

Defaults The domain field is not distinguished by default, and authenticated normally.

Command Mode VPDN-Group interface configuration mode

Usage Guide After domain authentication is enabled, this command content takes effect. Only the domain matching this information is identified, and another domain rule is used for the match in unmatched conditions. The authentication fails if no matched group is found.
Multiple domains can be configured in the same VPDN group and no upper limit of the domain quantity is set.
When no VRF is specified, this field corresponds to the global VRF.

Configuration Examples

The following example configures the inner header to belong to vrf1 after the ruijie.net domain is successfully authenticated.

```
Ruijie(config-vpdn)# domain ruijie.net vrf 1
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
vpdn authorize	Enables domain name split.
vpdn domain-delimiter	Configures domain name resolution.

Platform Description

N/A

force-local-chap

Use this command to force PPP to implement local CHAP authentication.

By default, when LAC is triggered on the client and dialup starts, LAC authenticates the client on behalf of LNS. Occsionally, LAC includes the CHAP authentication information on the client in an L2TP control packet sent to LNS. LNS resolves the PPP information sent from LAC and determines whether the PPP information is legal. If it is legal, LNS uses the information directly and skips CHAP authenticaton.

You can run this command to force LNS to authenticate the client again after L2TP tunnel establishment. This command is applicable only to LNS.

force-local-chap

no force-local-chap

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, LNS is not required to perform local CHAP authentication on the client after LNS receives PPP authentication information from LAC and determines that the information is legal.

Command Mode

VPDN-Group interface configuration mode

Usage Guide

After this command is executed, LNS ignores the PPP authentication information sent from LAC during tunnel establishment between LAC and LNS and is forced to perform CHAP authentication on the client again. This command is applicable only to LNS.

Configuration Examples

The following example configures PPP CHAP re-authentication for tunnels.

```
Ruijie(config-vpdn)# force-local-chap
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

force-local-lcp

Use this command to force PPP to implement local LCP negotiation.
By default, when LAC dialup is triggered on the client, LAC authenticates the client. Occsionally, LAC includes the PPP negotiation information on the client in an L2TP control packet sent to LNS. LNS resolves the PPP information sent from LAC and determines whether the PPP information is legal. If it is legal, LNS uses the information directly and skips LCP negotiation.
You can run this command to force LNS to authenticate the client again after L2TP tunnel establishment and ignores authentication ifnormation sent from LAC. This command is applicable only to LNS.
force-local-lcp
no force-local-lcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, LNS is not required to perform local LCP negotiation with the client after LNS receives PPP negotiation information from LAC and determines that the information is legal.

Command Mode

VPDN-Group interface configuration mode

Usage Guide

After this command is executed, LNS ignores the PPP negotiation information sent from LAC during tunnel establishment between LAC and LNS and is forced to perform LCP negotiation with the client again. This command is applicable only to LNS.

Configuration Examples

The following example configures PPP LCP re-authentication for tunnels.

```
Ruijie(config-vpdn)# force-local-lcp
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip precedence

Use this command to set the IP header priority field of the load tunnel.

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

ip precedence { *precedence-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }

no ip precedence

Parameter Description

Parameter	Description
precedence-value	Value of the priority field in the range from 0 to 7
critical	The value of the priority field is 5.
flash	The value of the priority field is 3.
flash-overrid	The value of the priority field is 4.
immediate	The value of the priority field is 2.
internet	The value of the priority field is 6.
network	The value of the priority field is 7.
priority	The value of the priority field is 1.
routine	The value of the priority field is 0.

Defaults

By default, the system sets the value of the IP header priority field of the load tunnel to 0, namely, **routine**.

Command Mode

VPDN-Group interface configuration mode

Usage Guide

Users can set the data priority of a tunnel with this command. Effective setting of this command will immediately affect transmission of data over the tunnel, but will not cause the related tunnel to be removed actively and forcibly. This command is applicable only to L2TP, not to PPTP.

Configuration Examples

The following example sets the priority of the tunnel data to 7.

```
Ruijie(config-vpdn)# ip precedence 7
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip tos

Use this command to set the IP header Type of Service (ToS) field of the load tunnel.

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

ip tos { *tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min- monetary-cost** | **normal** | **reflect** }

no ip tos

Parameter Description

Parameter	Description
tos-value	Value of the ToS field in the range from 0 to 15
max-reliability	The value of the ToS field is 2.
max-throughput	The value of the ToS field is 4.
min-delay	The value of the ToS field is 8.
min-monetary-cost	The value of the ToS field is 1.
normal	The value of the ToS field is 0.
reflect	Uses the ToS of the IP packet that the tunnel carries as the ToS field of the IP header of the load tunnel.

Defaults The default value of the IP header ToS field of the load tunnel is 0.

Command Mode VPDN-Group interface configuration mode

Usage Guide You can run this command to set the ToS of tunnel data. Effective setting of this command will immediately affect transmission of data over tunnels, but will not cause the related tunnel to be removed actively and forcibly. This command is applicable only to L2TP, but not to PPTP.

Configuration Examples The following example sets the ToS of tunnel data to **min-delay**.

```
Ruijie(config-vpdn)# ip tos min-delay
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

local name

Use this command to set the local host name of a tunnel.
Use the **no** form of this command to restore the default setting.
local name *local-hostname-string*
no local name

Parameter Description

Parameter	Description
local-hostname-string	Local host name of a tunnel

Defaults The system uses the name of a router as the local host name of a tunnel by default.

Command VPDN-Group interface configuration mode

Mode

Usage guideline

You can set the local host name of a tunnel on a router to identify the tunnel. Effective setting or change of this command will immediately cause the relevant existing tunnels to be removed actively and forcibly.

Configuration Examples

The following example sets the local host name of a tunnel to LNS.

```
Ruijie(config-vpdn)# local name LNS
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

pool

Use this command to set the address pool for the PPP protocol to assign peer addresses after tunnel negotiation is successful.
Use the **no** form of this command to restore the default setting.
pool *pool-name*
no pool

Parameter Description

Parameter	Description
pool-name	Address pool name

Defaults

The system does not specify any address pool for address assignment by default.

Command Mode

VPDN-Group interface configuration mode

Usage Guide

You can specify the bound address pool based on a domain name. After tunnel negotiation is successful, the system searches for the address pool based on the domain name and assigns an address in this pool to the peer.
The address pool on virtual-template interface is used if no address pool is specified. The name of an address pool supports up tp 30 bits.

Configuration Examples

The following example specifies the address pool named **vpdn** for user address assignment based on the domain name ruijie.

```
Ruijie(config-vpdn)# domain ruijie
Ruijie(config-vpdn-domain)# pool vpdn
Ruijie(config-vpdn-domain)#
```

Related

Command	Description

Commands	**domain**	Configures a user domain name.

Platform Description N/A

protocol

Use this command to set the tunnel protocol for a tunnel.
Use the **no** form of this command to restore the default setting.
protocol {any | l2tp | pptp}
no protocol

Parameter Description	**Parameter**	**Description**
	any	Matches all the available tunnel protocols.
	l2tp	Matches the tunnel protocol L2TP.
	pptp	Matches the tunnel protocol PPTP.

Defaults The system does not specify any configured tunnel protocol for a tunnel by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide Users must specify a tunnel protocol to be used by a tunnel. Any effective setting or change of the tunnel protocol will cause the related existing tunnels to be removed actively.

Configuration Examples The following example sets the tunnel protocol to L2TP.

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol l2tp
Ruijie(config-vpdn-acc-in)#
```

Related Commands	**Command**	**Description**
	domain	Configures a user domain name.

Platform Description N/A

source-ip

Use this command to set the local (source) address that the tunnel corresponding to the current VPDN-Group uses.
Use the **no** form of this command to restore the default setting.
source-ip *A.B.C.D*
no source-ip

Parameter Description

Parameter	Description
A.B.C.D	Local (source) address that the tunnel corresponding to the current VPDN-Group uses

Defaults

By default, the system does not specify the local (source) address that VPDN-Group uses when establishing a tunnel.

Command Mode

VPDN-Group interface configuration mode

Usage Guide

If the local (source) address used by the global VPDN function has been set, the local (source) address that VPDN-Group uses when establishing a tunnel must be consistent with it. Effective setting or change of this command will immediately cause the relevant existing tunnels to be removed actively and forcibly.

Configuration Examples

The following example sets the source address that the current VPDN-Group uses to 202.101.92.73.

```
Ruijie(config-vpdn)# source-ip 202.101.92.73
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

terminate-from

Use this command to specify the remote host name of a tunnel.
Use the **no** form of this command to restore the default setting.
terminate-from hostname *remote-hostname-string*
no terminate-from

Parameter Description

Parameter	Description
remote-hostname-string	Name of the remote host of a tunnel

Defaults

The remote host name of a tunnel is not set by default.

Command Mode

VPDN-Group interface configuration mode

Usage Guide

You can use this command to restrict the host name of the user who accesses remotely. If the remote host name of the tunnel is not set, VPDN-Group does not restrict the host name of the user who accesses remotely. Any effective change of the remote host name of the tunnel will cause all the existing tunnels corresponding to VPDN-Group where the tunnel is located to be

removed forcibly and actively.

Configuration Examples

The following example sets the remote host name of the tunnel to LAC.

```
Ruijie(config-vpdn)# terminate-from hostname LAC
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

virtual-template

Use this command to set the virtual template interface bound to the current VPDN-Group.
Use the **no** form of this command to restore the default setting.
virtual-template *number*
no virtual-template

Parameter Description

Parameter	Description
number	Serial number of the virtual template interface

Defaults

The system does not bind any virtual template interface to VPDN-Group by default.

Command Mode

VPDN-Group interface configuration mode

Usage Guide

You can use this command to bind the virtual template interface used by VPDN-Group to determine the parameters of the network interface that carries the session. If you want to provide VPDN-Group, you must bind the virtual template interface. Any effective change of the virtual template interface bound to VPDN- Group will cause the existing tunnels corresponding to this VPDN-Group to be removed forcibly.

Examples

The following example binds the virtual template interface 1 to VPDN-Group.

```
Ruijie(config-vpdn-acc-in)# virtual-template 1
Ruijie(config-vpdn-acc-in)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

vpdn-group

Use this command to set the VPDN-Group interface with the specified name. If the corresponding VPDN-Group interface does not exist, a VPDN-Group interface with the specified name will be created.
Use the **no** form of this command to delete a VPDN-Group interface with the specified name.
vpdn-group *vpdn-group-name*
no vpdn-group *vpdn-group-name*

Parameter description

Parameter	Description
vpdn-group-name	Name of the VPDN-Group interface

Defaults

The system does not set any VPDN-Group interface by default.

Command Mode

Global configuration mode.

Usage Guide

If you require a router to work as LNS or HGW, create and set a VPDN-Group interface. you can manage the VPDN-Group interface with this command. If the VPDN-Group interface is removed, the corresponding existing tunnels will be removed actively and forcibly.

Configuration Examples

The following example creates a VPDN-Group interface named **1**.

```
Ruijie(config)# vpdn-group 1
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

vpn

Use this command to set the VRF where the outer packets of a tunnel are located.
vpn vrf *vrf-name*
no vpn vrf

Parameter Description

Parameter	Description
vrf	Specifies the type as VRF.
vrf-name	Specifies the VRF name.

Defaults

The outer tunnel uses the global VRF by default, regardless of what VRF the interface belongs to.

Command Mode VPDN-Group interface configuration mode

Usage Guide If VRF has been configured on an interface without using this command, the tunnel will span the glocal VRF after encapsulation. If the spanning is not required, run this command to ensure that VPN VRF is consistent with IP VRF forward.

Configuration Examples The following command configures the outer header of a tunnel to belong to vrf1.

```
Ruijie(config-vpdn)# vpn vrf 1
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
ip vrf	Configures VRF.

Platform Description N/A

PPTP Commands

pptp flow-control receive-window

Use this command to define the maximum number of packets that the peer of the PPTP session can send before receiving the ACK packet from the local end, which is also referred to as the receiving window of the local end.
Use the **no** form of this command to restore the default setting.
pptp flow-control receive-window *packets*
no pptp flow-control receive-window

Parameter Description

Parameter	Description
packets	Maximum number of packets that the peer of the PPTP session can send before receiving the packet ACK message from the local end, in the range from 1 to 64

Defaults

The default value of PNS is 64, and that of PAC is 16.

Command Mode

VPDN-Group configuration mode

Usage Guide

This configuration command is exclusively used for the PPTP protocol. Therefore, users must first run the **protocol pptp** or **protocol any** command before running this command.
As specified in RFC2637, during negotiation, both parties of a session use half of the maximum receiving window received from the peer end as the initial sending window of the local end. When the sending window is full, no packets are sent to the peer end and the sending window is reduced by half until it reaches 1. Packets will be sent again when the ACK message is received from the peer end. If the timer for the ACK message does not time out after the number of packets sent continuously to the peer end reaches the size of the current window, then the size of the sending window at the local end is increased by 1 until it is equal to the value of the maximum receiving window at the peer end. According to RFC2637, the time of waiting for ACK timeout is calculated using a special algorithm.

Configuration Examples

The following example sets the value of the maximum receiving window of the PPTP session at the local end to 32.

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol pptp
Ruijie(config-vpdn-acc-in)# exit
Ruijie(config-vpdn)# pptp flow-control receive-window 32
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

pptp flow-control static-rtt

Use this command to define the static reference timeout period for waiting for the ACK response to a single packet that the PPTP session sends.
Use the **no** form of this command to restore the default setting.
pptp flow-control static-rtt *timeout-interval*
no pptp flow-control static-rtt

Parameter Description

Parameter	Description
packets	Static reference timeout period (in milliseconds) for waiting for the ACK response to a single packet that the PPTP session sends, in the range from 100 to 5000

Defaults The default value is 1500 milliseconds.

Command Mode VPDN-Group configuration mode

Usage Guide

This configuration command is exclusively used for the PPTP protocol. Therefore, users must first run the protocol pptp or protocol any command before running this command.
As specified in RFC2637, the interval of waiting for ACK timeout (ATO, Acknowledgment Time-Outs) after PPTP sends packets is calculated using a special algorithm, where the dynamically calculated round-trip time (RTT) is used. The time static-rtt configured in this command is used as a reference initial value for RTT calculation.

Configuration Examples

The following commands sets the value of the maximum receiving window of the PPTP session at the local end to 32.

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol pptp
Ruijie(config-vpdn-acc-in)# exit
Ruijie(config-vpdn)# pptp flow-control static-rtt 32
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

pptp tunnel echo

Use this command to set the time interval at which the PPTP tunnel actively sends an echo request.
Use the **no** form of this command to restore the default setting.

pptp tunnel echo *echo-packet-interval*

no pptp tunnel echo

Parameter Description

Parameter	Description
echo-packet-interval	Time interval (in seconds) at which the PPTP tunnel sends an echo request, in the range from 0 to 1000

Defaults

The default time interval is 60 seconds.

Command Mode

VPDN-Group configuration mode

Usage Guide

This configuration command is exclusively used for the PPTP protocol. Therefore, users must first run the **protocol pptp** or **protocol any** command before running this command. When *echo-packet-interval* is set to 0, the echo message is not sent actively.
When *echo-packet-interval* is not 0, if the PPTP tunnel does not receive any valid protocol or packet from the remote end for the *echo-packet-interval* consecutive seconds, it will actively send an echo request to detect the status of the tunnel and start timing and wait for the echo response from the remote end. The initial time of waiting for response is 1 second. If the first response times out, the tunnel immediately sends the second echo request and doubles the time of waiting for response, and so on. The tunnel communication is considered abnormal and the tunnel and its sessions will be closed if no echo reply is received from the remote end after five consecutive requests are sent.

Configuration Examples

The following example sets PPTP echo request to 30 seconds.

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol pptp
Ruijie(config-vpdn-acc-in)# exit
Ruijie(config-vpdn)# pptp tunnel echo 30
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

L2TP Commands

authentication (L2TP)

Use this command to enable the channel authentication function.

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

authentication

no authentication

Parameter Description

Parameter	Description
N/A	N/A

Defaults The channel authentication function is disabled by default.

Command Mode L2TP-Class interface configuration mode

Usage Guide You can enable or disable the channel authentication function as necessary. Any effective change to the setting of the channel authentication function will cause related tunnels of this L2TP-Class to be removed actively and forcibly.

Configuration Examples The following example enables the channel authentication function.

```
Ruijie(config-l2tp-class)# authentication
Ruijie(config-l2tp-class)#
```

Related Commands

Command	Description
Ruijie(config-l2tp-class)# **password** ***password****-string*	Sets the channel authentication password.

Platform Description N/A

encapsulation (L2TP)

Use this command to set the data encapsulation mode of tunnels.

encapsulation l2tpv2

Parameter Description

Parameter	Description
l2tpv2	Transmits tunnel data through L2TP configured in the RFC 2661 specifications.

Defaults The data encapsulation mode of tunnels is not set by default.

Command Mode Pseudowire-Class interface configuration mode

Usage Guide On the pseudowire-class interface, you must first set the tunnel data encapsulation mode before setting the tunnel data transmission parameters.

Configuration Examples The following example sets the tunnel data encapsulation mode to L2TPv2.

```
Ruijie(config-pw-class)# encapsulation l2tpv2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

hello

Use this command to set the interval of sending Hello messages to make the L2TP channel keepalive.

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

hello *interval*

no hello

Parameter Description

Parameter	Description
interval	Interval of sending Hello messages

Defaults Hello messages are sent at an interval of 60 seconds by default.

Command Mode L2TP-Class interface configuration mode

Usage Guide You can set the interval of sending Hello messages to check whether the L2TP channel is still available based on the network environment. If the network is stable, the interval of sending Hello messages can be set to a large value. Any effective change to the interval of sending Hello message will cause the corresponding existing L2TP tunnel to be removed actively and forcibly.

Configuration Examples The following example sets the interval of sending Hello messages to 120 seconds.

```
Ruijie(config-l2tp-class)# hello 120
Ruijie(config-l2tp-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

hostname (L2TP)

Use this command to set the local host name of the L2TP tunnel.
Use the **no** form of this command to restore the default setting.
hostname *local-hostname-string*
no hostname

Parameter Description	**Parameter**	**Description**
	local-hostname-string	Local host name of a tunnel

Defaults	The system uses the name of a router as the local host name of a tunnel by default.
Command Mode	L2TP-Class interface configuration mode
Usage Guide	You can set the local host name of a tunnel as necessary, so as to identify the tunnel. Any effective change to the local host name of the tunnel will cause the corresponding existing L2TP tunnel to be removed forcibly and actively.

Configuration Examples	The following example sets the local host name of a tunnel to LAC.
	`Ruijie(config-l2tp-class)# hostname LAC`
	`Ruijie(config-l2tp-class)#`

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

Platform Description	N/A

ip dfbit set

Use this command to disable tunnel data fragmentation for sending.
Use the **no** form of this command to restore the default value.
ip dfbit set
no ip dfbit set

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

Defaults The system allows tunnel data fragmentation for sending by default.

Command Mode Pseudowire-Class interface configuration mode

Usage Guide You can set whether to fragment tunnel data for sending as necessary. Any effective change to the setting of the tunnel data fragmentation function will immediately apply to transmission of the tunnel data, but will not cause the corresponding L2TP tunnel to be removed forcibly.

Configuration Examples The following example disables tunnel data fragmentation for sending.

```
Ruijie(config-pw-class)# ip dfbit set
Ruijie(config-pw-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip local interface

Use this command to set the local (source) interface of a tunnel.
Use the **no** form of this command to restore the default setting.
ip local interface *interface-name*
no ip local interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Local interface name

Defaults The system does not specify any local (source) interface to be used by a tunnel by default.

Command Mode Pseudowire-Class interface configuration mode

Usage Guide You can specify a router's network interface as the local (source) interface of a tunnel. Any effective change to the setting of the local (source) interface of a tunnel will cause the corresponding L2TP tunnel to be removed actively and forcibly.

Configuration Examples The following example sets the local (source) interface of a tunnel to Serial 0.

```
Ruijie(config-pw-class)# ip local interface serial 0
Ruijie(config-pw-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip ttl

Use this command to set the **TTL** field in the IP header of load tunnel data.
Use the **no** form of this command to restore the default setting.
ip ttl *ttl-value*
no ip ttl

Parameter Description

Parameter	Description
ttl-value	Value of the TTL field in the range from 1 to 255

Defaults The **TTL** field in the IP header of load tunnel data is set to 255 by default.

Command Mode Pseudowire-Class interface configuration mode

Usage Guide You can set the **TTL** field in the IP header of the data over the load tunnel as necessary. Any effective change to the setting of the field will immediately apply to transmission of the data over the tunnel, but will not cause the corresponding L2TP tunnel to be removed forcibly.

Configuration Examples The following example sets the value of the **TTL** field in the IP header of the data over the load tunnel to 253.

```
Ruijie(config-pw-class)# ip ttl 253
Ruijie(config-pw-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp-class

Use this command to set an L2TP-class interface with the specified name. If no interface with the specified name exists, an L2TP-class interface with the specified name is created.
Use the **no** form of this command to remove the l2tp-class interface with the specified name.
l2tp-class *l2tp-class-name*

no l2tp-class *l2tp-class-name*

Parameter Description	Parameter	Description
	l2tp-class-name	Name of an L2TP-Class interface

Defaults The system does not set any L2TP-Class interface by default.

Command Mode Global configuration mode

Usage Guide You can set the working parameters of the L2TP control connection by configuring and referencing L2TP-Class.

Configuration Examples The following example creates an L2TP-Class interface named l2x:

```
Ruijie(config)# l2tp-class l2x
Ruijie(config-l2tp-class)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

l2tp ip udp checksum

Use this command to set the **Checksum** field of the UDP packet of the load tunnel.
Use the **no** form of this command to restore the default setting.
l2tp ip udp checksum
no l2tp ip udp checksum

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The system requires that the **Checksum** field of the UDP packet of the load tunnel be null (namely, 0) by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide You can set whether to require the UDP packet of the load tunnel data to calculate and fill in the **Checksum** field. Any effective change to the setting of the field will immediately apply to transmission of the data over the tunnel, but will not cause the corresponding L2TP tunnel to be removed forcibly.

Configuration Examples The following example requires the UDP packet of the load tunnel to set the **Checksum** field.

```
Ruijie(config-vpdn)# l2tp ip udp checksum
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel authentication

Use this command to enable the channel authentication function.

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

l2tp tunnel authentication

no l2tp tunnel authentication

Parameter Description

Parameter	Description
N/A	N/A

Defaults The channel authentication function is disabled by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide You can enable or disable the channel authentication function as necessary. Any effective change to the setting of the channel authentication function will cause related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example enables the channel authentication function.

```
Ruijie(config-vpdn)# l2tp tunnel authentication
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel avp-hidden-compatible

Use this command to support the AVP Hidden resolution algorithm of the RFC2661 standard. The AVP Hidden resolution algorithm of the Cisco standard is supported by default.
Use the **no** form of this command to restore the default setting.
l2tp tunnel avp-hidden-compatible
no l2tp tunnel avp-hidden-compatible

Parameter Description

Parameter	Description
N/A	N/A

Defaults The AVP Hidden resolution algorithm of the Cisco standard is used by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide You can enable or disable compatibility of the RFC2661 AVP Hidden resolution algorithm as necessary. You can configure multiple VPDN-Groups to support the RFC2661 and Cisco AVP Hidden resolution algorithms. Execution of this command does not affect the existing L2TP tunnel.

Configuration Examples The following example configures compatibility of the RFC2661 AVP Hidden resolution function.

```
Ruijie(config-vpdn)# l2tp tunnel avp-hidden-compatible
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel force_ipsec

Use this command to configure usage with IPSec in external encryption mode, in which only encrypted packets can pass over VPDN tunnels.
Use the **no** form of this command to restore the default setting.
l2tp tunnel force_ipsec
no l2tp tunnel force_ipsec

Parameter Description

Parameter	Description
N/A	N/A

Defaults Forcible packet encryption is disabled by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide You can enable or disable forcible encryption as necessary, Any effective change to the setting of the channel authentication function will cause related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example enables forcible encryption.

```
Ruijie(config-vpdn)# l2tp tunnel force_ipsec
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel hello

Use this command to set the interval of sending Hello messages to make a channel keepalive. Use the **no** form of this command to restore the default setting.

l2tp tunnel hello *interval*

no l2tp tunnel hello

Parameter Description

Parameter	Description
interval	Interval (in seconds) of sending Hello messages

Defaults The interval of sending Hello messages is set to 60 seconds by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide You can set the interval of sending Hello messages based on the network environments as necessary. Any effective change to the setting of the interval of sending Hello messages for a channel will cause the corresponding L2TP tunnel to be removed actively and forcibly.

Configuration Examples The following example sets the interval of sending Hello messages to 30 seconds.

```
Ruijie(config-vpdn)# l2tp tunnel hello 30
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel password

Use this command to set a password of channel authentication.

Use the **no** form of this command to clear the password of channel authentication.

l2tp tunnel password *password-string*

no l2tp tunnel password

Parameter Description

Parameter	Description
password-string	Password of channel authentication

Defaults No password of channel authentication is set by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide If you need to authenticate a channel, enable the channel authentication function at both ends of the tunnel and use the same authentication password. Any effective change to the setting of the channel authentication password will cause related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the channel authentication password to share:

```
Ruijie(config-vpdn)# l2tp tunnel password share
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel receive-window

Use this command to set the size of the channel control message receiving window.

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

l2tp tunnel receive-window *size*

no l2tp tunnel receive-window

Parameter Description

Parameter	Description
size	Size of the channel control message receiving window

Defaults The default size of the channel control message receiving window is 4.

Command Mode VPDN-Group interface configuration mode

Usage Guide Any effective change to the setting of the size of the channel control message receiving window will cause the related L2TP tunnels to be removed forcibly.

Configuration Examples The following example sets the size of the control message receiving window to 12.

```
Ruijie(config-vpdn)# l2tp tunnel receive-window 12
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel retransmit

Use this command to set the retransmission parameters of the L2TP channel control message.
Use the **no** form of this command to restore the default setting.
l2tp tunnel retransmit {**retries** *number* | **timeout** { **min** | **max** } *seconds* }
no l2tp tunnel retransmit { **retries** | **timeout** { **min** | **max** } }

Parameter Description

Parameter	Description
number	Retransmission times of control messages
seconds	Interval of control message retransmission

Defaults By default, the maximum retransmission times of control messages are 5, the minimum interval of control message retransmission is 1 seconds, and the maximum interval is 8 seconds.

Command Mode VPDN-Group interface configuration mode

Usage Guide Any effective change to the setting of retransmission parameters of the channel control message will cause related L2TP tunnels to be removed actively and forcibly.

Configuration The following example sets the maximum retransmission times of control messages to 10.

Examples

```
Ruijie(config-vpdn)# l2tp tunnel retransmit retries 10
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

l2tp tunnel timeout

Use this command to set the maximum period of no session/control connection that L2TP allows. Use the **no** form of this command to restore the default setting.

l2tp tunnel timeout {**no-session**| **setup**} *seconds*

no l2tp tunnel timeout {**no-session** | **setup**}

Parameter Description

Parameter	Description
no-session	Sets the status where the channel has been set up, but the session has not been set up.
setup	Sets the status where the control connection (channel) has not been set up.
seconds	Time interval, in seconds

Defaults By default, the maximum period of no session that the system allows is 600 seconds, and the maximum time that the system allows for setting up a control connection (channel) is 300 seconds.

Command Mode VPDN-Group interface configuration mode

Usage Guide Any effective change to the setting of the maximum time interval of no session/control connection setup that the existing channel allows will cause the related L2TP tunnels to be removed forcibly and actively.

Configuration Examples The following example sets the time interval of no session that the channel allows to 1200 seconds.

```
Ruijie(config-vpdn)# l2tp tunnel timeout no-session 1200
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

l2tp tunnel zxkeepalive-compatible

Use this command to enable the L2TP LNS to return SCCRP packets without Challenge Response AVP 13 when receiving SCCRQ packets without Challenge AVP 11 after tunnel authentication is configured. Use the **no** form of this command to disable this function.

l2tp tunnel zxkeepalive-compatible

no l2tp tunnel zxkeepalive-compatible

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, L2TP LNS returns the SCCRP packet containing challenge response AVP13 and all-zero return value after receiving SCCRQ packets without Challenge AVP 11

Command Mode

VPDN-Group interface configuration mode

Usage Guide

This command is used with the **l2tp tunnel authentication** command.

Configuration Examples

The following example returns SCCRP packets without the challenge response AVP upon receiving SCCRQ packets without the challenge AVP.

```
Ruijie(config-vpdn)# l2tp tunnel zxkeepalive-compatible
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

lcp renegotiation always

Use this command to ingore the received error of L2TP control packets that do not comply with RFC specifications to ensure normal negotiation.

lcp renegotiation always

no lcp renegotiation always

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The received L2TP control packets must strictly comply with RFC specifications by default.

Command Mode VPDN-Group interface configuration mode

Usage Guide N/A

Configuration Examples The following example ignores all control word errors that do not comply with RFC.

```
Ruijie(config-vpdn)# lcp renegotiation always
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

password (L2TP)

Use this command to set a password of channel authentication.
Use the **no** form of this command to restore the default setting.
password *password-string*
no password

Parameter Description

Parameter	Description
password-string	Password of channel authentication

Defaults No password of channel authentication is set because the system disables the channel authentication function by default.

Command Mode L2TP-Class interface configuration mode

Usage Guide If you need to authenticate a channel, enable the channel authentication function at both ends of the tunnel and use the same authentication password. Any effective change to the setting of the channel authentication password will cause related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the channel authentication password to **share**.

```
Ruijie(config-l2tp-class)# password share
Ruijie(config-l2tp-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

protocol (L2TP)

Use this command to set the L2TP control connection parameters.
Use the **no** form of this command to restore the default setting.
protocol l2tpv2 [*l2tp-class-name*]
no protocol

Parameter Description

Parameter	Description
l2tpv2	Uses L2TP as the tunneling protocol.
l2tp-class-name	Name of the L2TP-Class interface

Defaults L2TPv2 is used as the L2TP tunneling protocol by default.

Command Mode Pseudowire-Class interface configuration mode

Usage Guide Any effective change to the setting of the control connection parameters will cause related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the tunneling protocol to L2TPv2 and uses L2TP-Class l2x to set control connection parameters.

```
Ruijie(config-pw-class)# protocol l2tpv2 l2x
Ruijie(config-pw-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

pseudowire

Use this command to set pseudowire rules.
Use the **no** form of this command to restore the default setting.
pseudowire *peer-ip-address vcid* { **encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }
no pseudowire
Configure the pseudowire with the **hostname** parameter.
pseudowire hostname *peer-hostname vcid* { **encapsulation l2tpv2** [**pw-class**

pw-class-name] | **pw-class** *pw-class-name* }

no pseudowire

Parameter Description

Parameter	Description
peer-ip-address	Address of the remote L2TP server (LNS)
peer-hostname	Host name of the remote L2TP server (LNS) registered on the DNS and corresponding to other addresses
vcid	Global labeled amount of the the pseudowire
l2tpv2	Uses L2tpv2 (RFC 2661) as the tunneling protocol.
pw-class-name	Name of the referenced pseudowire-class unit

Defaults No pseudowire rule is set by default.

Command Mode Interface configuration mode

Usage Guide The pseudowire rule can be configured only on the virtual-PPP interface. Any effective change to the pseudowire rule on the virtual-ppp interface will cause related L2TP sessions to be removed actively and forcibly.

Configuration Examples The following example sets the pseudowire rule on the virtual-PPP interface, with the LNS address set to 192.168.12.213 and the pseudowire-class interface pw being referenced

```
Ruijie(config)# interface virtual-ppp 1
Ruijie(config-if)# pseudowire 192.168.12.213 33 pw-class pw
Ruijie(config-if)#
```

Host name configuration :

The following example enables the DNS service, configures the DNS address, and configures a route to the server.

```
ip domain-lookup
l2tp-class 1
pseudowire-class 1
 encapsulation l2tpv2
ip name-server 192.168.5.119
ip name-server 61.154.22.41
interface FastEthernet 0/0
 ip ref
 ip address 192.168.52.90 255.255.255.0
 duplex auto
 speed auto
interface Virtual-ppp 1
 pseudowire hostname mm.hxs.meibu.com 1 encapsulation l2tpv2
 ppp pap sent-username user1 password  11
 ip address negotiate
ip route 0.0.0.0 0.0.0.0 192.168.52.1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

pseudowire-class

Use this command to set a pseudowire-class interface with the specified name. If no pseudowire-class interface with the specified name exists, a pseudowire-class interface with the specified name is created.
Use the **no** form of this command to remove the pseudowire-class interface with the specified name.
pseudowire-class *pseudowire-class-name*
no pseudowire-class *pseudowire-class-name*

Parameter Description	Parameter	Description
	pseudowire-class-name	Name of the pseudowire-class interface

Defaults No pseudowire-class interface is set by default.

Command Mode Global configuration mode

Usage Guide You can set the working parameters of the L2TP tunnel by configuring and referencing the pseudowire-class interface.

Configuration Examples The following example creates a pseudowire-class interface named pw.

```
Ruijie(config)# pseudowire-class pw
Ruijie(config-pw-class)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

receive-window

Use this command to set the size of the tunnel control message receiving window.
Use the **no** form of this command to restore the default setting.
receive-window *size*

no receive-window

Parameter Description

Parameter	Description
size	Size of the control message receiving window

Defaults The default size of the control message receiving window is 8.

Command Mode L2TP-Class interface configuration mode

Usage Guide Any effective change to the size of the tunnel control message receiving window will cause the related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the size of the control message receiving window to 12.

```
Ruijie(config-l2tp-class)# receive-window 12
Ruijie(config-l2tp-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

retransmit

Use this command to set the retransmission parameters of the control message.
Use the **no** form of this command to restore the default setting.
retransmit { **initial** { **retries** *initial-retries* | **timeout** { **max** | **min** } *initial-timeout* } | **retries** *retries* | **timeout** { **max** | **min** } *timeout* }
no retransmit { **initial** { **retries** | timeout { **max** | **min** } } | **retries** | **timeout** { **max** | **min** } }

Parameter Description

Parameter	Description
initial-retries	SCCRQ retransmision times
initial-timeout	Time interval of SCCRQ retransmision
retries	Retransmision times of other control messages
timeout	Time interval of retransmitting other control messages

Defaults By default, the SCCRQ retransmision times are 2, the retransmision times of other control messages is 5, the minimum time interval of transmitting control message is 1 second, and the maximum time interval of transmitting control message is 8 seconds.

Command Mode L2TP-Class interface configuration mode

Usage Guide Any effective change to the setting of the retransmission parameters of the control message will cause related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the SCCRQ retransmision times to 3.

```
Ruijie(config-l2tp-class)# retransmit initial retries 3
Ruijie(config-l2tp-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

timeout setup

Use this command to set the maximum time that the system allows for setting up a control connection.

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

timeout setup *seconds*

no timeout setup

Parameter Description

Parameter	Description
seconds	Maximum time (in seconds) that the system allows for setting up a control connection

Defaults The maximum time that the system allows for setting up a control connection is 300 seconds by default.

Command Mode L2TP-Class interface configuration mode

Usage Guide Any effective change to the maximum time that the system allows for setting up a control connection will cause related L2TP tunnels to be removed actively and forcibly.

Configuration Examples The following example sets the maximum time that the system allows for setting up a control connection to 240 seconds.

```
Ruijie(config-l2tp-class)# timeout setup 240
Ruijie(config-l2tp-class)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn vrf

Use this command to set the VRF where the L2TP tunnel's outer header is located.

vpdn vrf *vrf-name*

no vpdn vrf

Parameter Description

Parameter	Description
vrf	Specifies the type as VRF.
vrf-name	VRF name

Defaults The outer tunnel uses the global VRF by default no matter which VRF the interface belongs to.

Command Mode Interface configuration mode

Usage Guide This command is visible only on the Virtual-PPP interface and can be executed only on the L2TP tunnel.

If the VRF has been configured on the interface without this command executed, the tunnel will span the global VRF after encapsulation. If the spanning is not required, you need to run this command to ensure consistency between the VPN VRF and IP VRF forward.

Configuration Examples The following example sets the tunnel's outer header to belong to VRF1.

```
Ruijie(config-Virtual-ppp 1)#vpdn vrf 1
Ruijie(config-Virtual-ppp 1)#
```

Related Commands

Command	Description
ip vrf	Configures the VRF.

Platform Description N/A

VPDN 2.0 Commands

domain

Use the following command to set group's related domain field content, and apply it for the domain authentication of version VPDN 2.0.

domain *domain-name* [**virtual-vpdn** *number*]

no domain *domain-name*

Parameter Description

Parameter	Description
domain-name	Domain name.
virtual-vpdn	Logical interface binded with specified session.
number	Logical interface number <1-1024>

Defaults The domain field is not distinguished by default, and authenticated normally.

Command Mode VPDN-Group interface configuration mode

Usage Guide After domain authentication is enabled, this command content takes effect. The command will also traversal all the domain configuration in the group. The match will negotiate following the domain rule. Only the matched domain is found, can a negotiation pass.
Multiple domains can be configured in the same VPDN group and no upper limit of the domain quantity is set.
When no virtual-vpdn interface is specified, use default interface to bind session.
The command can be seen only after the virtual-vpdn is configured in the group.

Configuration Examples Bind session with virtual-vpdn 1 interface after the ruijie.net domain is successfully authenticated.

```
Ruijie(config-vpdn)# domain ruijie.net virtual-vpdn 1
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
vpdn authorize	Enables domain name split.
vpdn domain-delimiter	Configures domain name resolution.

Platform Description N/A

Command History

Version Number	Description
10.3（5）	The first version that supports the command.
10.4(3b21)	Version with added virtual-vpdn command.

flow-label

Use this command to configure flow-limit QOS rule. Use the **no** form of this command to restore the default setting.

flow-label *number*

no flow-label

Parameter Description

Parameter	Description
number	Flow lable ID, in the range from 1 to 1023.

Defaults Flow limit is disabled by default.

Command Mode VPDN-Group interface configuration mode/domain configuration mode

Usage Guide Flow limit is supported by the tunnel bound with the virtual-vpdn interface.

Configuration Examples The following example sets a flow-limit QOS rule.

```
Ruijie(config-vpdn)# flow-label 1
Ruijie(config-vpdn)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

virtual-vpdn

Use this command to set a virtual-vpdn interface. Use the **no** form of this command to restore the default setting.

virtual-vpdn *number*

no virtual-vpdn

Parameter Description

Parameter	Description
number	Interface ID, in the range from 1 to 1024.

Defaults No virtual-vpdn interface is set by default.

Command Mode VPDN-Group interface configuration mode/domain configuration mode

Usage Guide The created virtual-vpdn interface will be used as the logical interface that binds and carries L2TP sessions. When negotiating tunnels by using virtual-vpdn interface, the L2TP tunnel does not support IPV6 negotiation. All the PPP authentication of virtual-vpdn interface in vpdn-group's domain configuration need to be configured on the default virtual-vpdn interface of vpdn-group.

Configuration Examples The following example sets virtual-vpdn interface 1.

```
Ruijie(config-vpdn-acc-in)# virtual-vpdn 1
Ruijie(config-vpdn-acc-in)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn intf_pool

Use this command to bind an address pool to a virtual-vpdn interface. Use the **no** form of this command to restore the default setting.

vpdn intf_pool *pool-name*

no vpdn intf_pool

Parameter Description

Parameter	Description
intf_pool	Specifies an interface pool.
pool-name	A pool name.

Defaults No address pool is bound to the virtual-vpdn interface by default.

Command Mode Interface configuration mode

Usage Guide The VPDN address pool can only be bound to the virtual-vpdn interface of L27P module.
This command must be configured after the vpdn-pool is configured globally. If the global vpdn-pool is deleted, this command will be deleted.

Configuration Examples The following example binds address pool ruijie to virtual-vpdn1.

```
Ruijie(config-vpdn-acc-in)# vpdn intf_pool ruijie
Ruijie(config-vpdn-acc-in)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpdn pool

Use this command to create a VPDN address pool. Use the **no** form of this command to restore the default setting.
vpdn pool *pool_name first-ip last_ip*
no vpdn pool *pool_name*

Parameter Description

Parameter	Description
pool_name	A pool name (64 characters max).
first-ip	The start IP address of the address pool.
last-ip	The end IP address of the address pool.

Defaults No VPDN address pool is configured by default.

Command Mode Global configuration mode

Usage Guide The VPDN address pool can only be bound to the virtual-vpdn interface of L27P module.
This command must be configured after the vpdn-pool is configured globally. If the global vpdn-pool is deleted, this command will be deleted.

Configuration Examples The following example sets VPDN address pool Ruijie from 11.1.1.1 to 11.1.1.250.

```
Ruijie(config-vpdn-acc-in)# vpdn pool ruijie 11.1.1.1 11.1.1.250
Ruijie(config-vpdn-acc-in)#
```

The following example sets VPDN address pool Ruijie from 11.1.1.1 to 11.1.1.250 and binds it to devid 4.

```
Ruijie(config)# vpdn pool ruijie 11.1.1.1 11.1.1.250 devid 4
Ruijie(config)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

IP NAT Commands

address

Use this command to configure the address range of an empty NAT address pool in NAT address pool configuration mode.
Use the **no** form of this command to delete the address range of an address pool.
address *start-ip end-ip* [**match interface** *interface*]
no address *start-ip end-ip* [**match interface** *interface*]
address interface *interface* [**match interface** *interface*]
no address interface *interface* [**match interface** *interface*]

Parameter Description

Parameter	Description
start-ip	Start IP address of an address block
end-ip	End IP address of an address block
interface *interface*	Sets the interface used when NAT has multiple outside interfaces. The addresses defined in a pool use interface addresses and are used when the interface addresses are unknown and will be negotiated. Note that this parameter must be used with the **match interface** interface parameter, and the two interfaces must be consistent. Otherwise, NAT may fails.
match interface *interface*	Sets the interface used when NAT has multiple outside interfaces. When the router determines the egress of packets, NAT uses this egress to select an address that matches it from the pool.

Defaults No address range is defined by default.

Command Mode NAT address pool configuration mode

Usage Guide If you need to define multiple address ranges for an address pool, first enter NAT address pool configuration mode, and then define the NAT address ranges.


Note

The **match** keyword is not available for the NPE80. That is, the comand format is as follows: **address** *start-ip end-ip* **match interface** *interface*
no address *start-ip end-ip* **match interface** *interface*
address interface *interface* **match interface** *interface*
no address interface *interface* **match interface** *interface*

Configuration Examples The following example creates a mulnets address pool and defines two address blocks.

```
ip nat pool mulnets netmask 255.255.255.0
address 172.16.10.1 172.16.10.254
address 192.168.100.1 192.168.100.50
```

Related Commands

Command	Description
ip nat pool	Defines the IP NAT address pool.

Platform Description N/A

clear ip nat statistics

Use this command to clear IP NAT statistics.

clear ip nat statistics rule

Parameter Description

Parameter	Description
rule	NAT rules

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you run this command, the IP NAT statistics on the line card will also be deleted.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear ip nat translation

Use this command in privileged EXEC mode to clear translation entries from the NAT table.

clear ip nat translation { ***** }

Parameter Description

Parameter	Description
*	Deletes all dynamic NAT entries.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to forcibly delete translation entries from the NAT table. Note that deleting all the NAT entries will affect the current sessions and may cause loss of connections such as FTP. Therefore, this operation should be performed with caution.

Configuration Examples N/A

Related Commands

Command	Description
ip nat	Performs NAT on the traffic that passes an interface.
ip nat inside destination	Enables NAT for the internal destination address.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool.
show ip nat statistics	Displays statistics on IP NAT.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

ip nat

Use this command to perform NAT on the incoming and outgoing traffic of an interface in interface configuration mode.
Use the **no** form of this command to disable NAT on an interface.
ip nat { **inside** | **outside** }
no ip nat { **inside** | **outside** }

Parameter Description

Parameter	Description
inside	Perfoms NAT on incoming packets.
outside	Performs NAT on outgoing packets.

Defaults NAT is not performed on the incoming and outgoing data of an interface by default.

Command Mode Interface configuration mode

Usage Guide NAT is performed only when packets are routed between outside and inside interfaces and meet a certain rule. Therefore, at least an inside interface and an outside interface must be configured for a router.

Configuration Examples The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```
!
interface FastEthernet0
ip address 192.168.12.6 255.255.255.0
ip nat inside
!
interface FastEthernet1
ip address 200.168.12.17 255.255.255.240
ip nat outside
!
ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
ip nat inside source list 1 pool net200
!
access-list 1 permit 192.168.12.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat inside destination	Enables NAT for the internal destination address.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

ip nat application

Use this command to implement special application of NAT in global configuration mode.
Use the **no** form of this command to cancel this special application.
ip nat application source list *list-num* **destination** *dest-ip*
{ **dest-change** | **src-change** } *ip-addr* [**vrf** vrf_*name*]
ip nat application source list *list-num* **destination** { **tcp** | **udp**
dest-ip port-num} { **dest-change** *ip-addr port-num* | **src-change**
ip-addr } [**vrf** vrf_*name*]
no ip nat application source list *list-num* **destination** *dest-ip*
{ **dest-change** | **src-change** } *ip-addr* [**vrf** vrf_*name*]

no ip nat application source list *list-num* **destination** { **tcp** | **udp** *dest-ip port-num*} { **dest-change** *ip-addr port-num* | **src-change** *ip-addr* } [**vrf** vrf_*name*]

Parameter Description

Parameter	Description
list-num	Access list of internal local addresses, that is, match criteria of the source addresses of packets
dest-ip	Internal global address match, that is, match criteria of the destination addresses of packets. NAT entries are created only when the destination IP address matches this address and the source IP address matches the previously defined access list.
tcp *dest-ip port-num*	Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the TCP packet match the criteria defined here and the source address matches the previously defined access list.
udp *dest-ip port-num*	Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the UDP packet match the criteria defined here and the source address matches the previously defined access list.
dest-change *ip-addr port-num*	Changes the destination address and port of the packet that meets criteria.
src-change *ip-addr*	Changes the source address of the packet that meets criteria.
vrf vrf_*name*	VRF name, which is effective in this VRF

Defaults This rule is not defined by default.

Command Mode Global configuration mode (this command is not supported on the NPE80)

Usage Guide In some advanced applications of NAT, it is necessary to change the source or destination addresses of some particular IP packets. This command can be used to perform this operation. The following example uses this command to implement the domain name resolution relay service (DNS relay). Note that this command is only applicable on routers.

Configuration Examples The following example allows the host in the network segment 192.168.1.0 in the internal network to point the DNS server to the IP address 192.168.1.1 of the NAT inside interface. The NAT function of the router forwards the DNS request from the host in the internal network to the true DNS server 202.101.98.55, and forwards the DNS response packet to the host in the internal network. Implement this function with the **ip nat application** command. The semantics is: If there is a UDP packet whose source address meets the criteria of access-list 1, destination address is 192.168.1.1,

and destination port is 53, then change the destination address of this IP packet to 202.101.98.55 and the destination port to 53. The script is as follows:

```
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
interface FastEthernet 0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
!
interface FastEthernet 1/0
ip address 200.168.12.1 255.255.255.0
ip nat outside
!
ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0
!
ip nat inside source list 1 pool net200
ip nat application source list 1 destination udp 192.168.1.1 53 dest-change
202.101.98.55 53
!
```

Related Commands

Command	Description
address	Defines the address block range of an address pool.
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed on the traffic that passes this interface.
ip nat inside destination	Enables NAT for the internal destination address.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

ip nat arp reply

Use this command to enable the ARP response function of NAT on the slave device.

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

ip nat arp reply

no ip nat arp reply

Parameter Description

Parameter	Description
N/A	N/A

Defaults ARP response packet is not sent by the slave device by default.

Command Mode Global configuration mode.

Usage Guide In the VRRP dual-node hot backup scenario, if the same NAT function is configured on both the master and slave devices, when the router initiates an ARP request, both devices receive the ARP request and return an ARP response, causing an ARP conflict. Therefore, the slave device does not respond to the ARP request by default. If NAT configurations on the master and slave devices are different, sometimes the slave device needs to respond to the ARP request. In this case, you can run the ip nat arp reply command, so that the slave device returns a response packet when receiving an ARP request.

Configuration Examples The following example configures NAT to enable the slave device to send ARP response packet.

```
Ruijie(config)#ip nat arp reply
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip nat inside destination

Use this command to enable NAT for the internal destination address in global configuration mode. Use the **no** form of this command to disable NAT for the internal destination address.

ip nat inside [**vrf** vrf_*name1*] **destination list** *access-list-number* **pool** *pool-name* [**vrf** vrf_*name2*]

no ip nat inside [**vrf** vrf_*name1*] **destination list** *access-list-number* **[pool** *pool-name***]** [**vrf** vrf_*name2*]

Parameter Description

Parameter	Description
list *access-list-number*	Internal global addresses are defined in the access list. If the external network accesses the address in the access list, the internal global address will be translated into the internal local address defined in the pool. Note that here you should use the extended ACL in the range from 100 to 199 whose destination IP address is a virtual IP address.
pool *pool-name*	A space in the address pool that defines the internal local address. An internal local address will be assigned from this space during destination address translation.
vrf *vrf_name1*	The packets sent from the vrf_name1 are effective.
vrf *vrf_name2*	Vrf name, which is effective in this VRF

Defaults Internal source address translation is disabled by default.

Command Mode Global configuration mode.

Usage Guide Translation of internal destination addresses can be performed to realize load balance of TCP traffic. When a host in the internal network is overloaded with TCP traffic, multiple hosts may be required to balance the load of TCP traffic. In this case, you can use NAT to realize load balance of TCP traffic. NAT will create a virtual host to provide the TCP service. This virtual host corresponds to multiple real internal hosts. Then, NAT polls and replaces the destination address, so as to distribute the load. However, no change is made to other IP traffic, unless NAT is configured otherwise.

When NAT is configured to realize TCP load balance, the address of the internal network can be either a valid global address or a private network address. However, the address of the virtual host must be a valid global address.

Configuration Examples The following example configures the internal network to provide a virtual host address 10.10.10.100 externally. The external network uses this address to access the WWW service. The hosts that provide services in the internal LAN are actually two hosts with the addresses 10.10.10.1 and 10.10.10.2. During NAT, load balance is realized in polling mode.

```
!
interface FastEthernet0
ip address 10.10.10.254 255.255.255.0
ip nat inside
!
interface FastEthernet1
ip address 200.168.12.17 255.255.255.240
ip nat outside
!
ip nat pool net10 10.10.10.1 10.10.10.2 prefix-length 24 type rotary
ip nat inside destination list 100 pool net10
!
access-list 100 permit ip any host 10.10.10.100
```

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed on the traffic that passes this interface.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enable NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool
show ip nat translations	Displays IP NAT entries.

Platform

Description N/A

ip nat inside source

Use this command to enable NAT for internal source addresses in interface configuration mode.
Use the **no** form of this command to disable static or dynamic NAT.

ip nat inside [**vrf** vrf_*name1*] **source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**] [**vrf** vrf_*name*]

no ip nat inside [**vrf** vrf_*name1*] **source list** *access-list-number* [**vrf** vrf_*name*]

ip nat inside [**vrf** vrf_*name1*] **source static** *local-ip global-ip* [**permit-inside**] [**vrf** vrf_*name*]

no ip nat inside [**vrf** vrf_*name1*] **source static** *local-ip global-ip* [**permit-inside**] [**vrf** vrf_*name*]

ip nat inside [**vrf** vrf_*name1*] **source static** *protocol local-ip local-port global-ip global-port* [**permit-inside**] [**vrf** vrf_*name2*]

no ip nat inside [**vrf** vrf_*name1*] **source static** *protocol local-ip local-port global-ip global-port* [**permit-inside**] [**vrf** vrf_*name2*]

Parameter Description

Parameter	Description
list *access-list-number*	Specifies the access list of local addresses. NAT entries will be created only for the traffic with the source address that matches this access list.
interface *interface-type interface-number*	Uses the global address of the outside interface to perform Network Address Port Translation (NAPT), also called extended NAT.
pool *pool-name*	Uses a global address in the address pool to perform NAT.
overload	(Optional) Every global address in the pool can be reused for translation, namely, NAPT. Currently, this parameter is not set, and global addresses are reusable. This parameter is added in order to be compatible with the command of Cisco.
static *local-ip global-ip*	Defines the simple static NAT. *local-ip* is a local address, and *global-ip* is a global address. The **no** form of this command does not check the validity of *global-ip*.
static *protocol*	Defines the extended static NAT. *protocol* can be either TCP or UDP.
local-port	Service port number (TCP or UDP) of the local address. Each service typically corresponds to a service port.
global-port	Service port number of the global address. The external network accesses the services of hosts in the internal network through this port. This port number can be different from *local-port*.

permit-inside	Allow users in the internal network to access the host with the IP address indicated by local-ip through global-ip. This keyword appears only in the **ip nat inside source static** command is applicable only on routers.
vrf *vrf_name1*	The packets sent from the vrf_name1 are effective.
vrf *vrf_name2*	VRF name, which is effective in this VRF.

Defaults NAT for internal source addresses is disabled by default.

Command Mode Global configuration mode

Usage Guide When the IP address of the internal network is a private address and the internal network needs to communicate with the external network, NAT must be configured to translate the internal private IP address into the globally unique IP address.

If organizations, such as net bars or enterprises, access the network only for obtaining resources in the external network, such as browsing Web pages, receiving and sending emails, and downloading files, but not for providing network services for the external network, the IP address of the outside interface can be used directly as the global address and the address is translated in NAPT mode. If NAT is not configured, the internal network with the private address, even if physically interconnected with the external network, is unable to interwork with the external network, because the external network does not provide network routing for the private address.

Static NAT or NAPT should be configured for the internal hosts that provide services. To ensure continuous service provisioning, do not use the address of the outside interface to perform NAPT because this address is interconnected with ISP and is very likely to be translated. Generally, users in the internal network can access the services provided by these internal hosts simply by using the IP address of the internal network. However, some special application services can only be accessed by users in the internal network using the global IP address. In this case, you need to add the keyword **permit-inside** when configuring static NAT or static NAPT for internal source addresses. Moreover, it is advisable to run the **no ip redirects** command on the inside interfae to prevent the inside interface from sending redirection packets.

Configuration Examples The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```
!
interface FastEthernet0
ip address 192.168.12.6 255.255.255.0
ip nat inside
!
interface FastEthernet1
ip address 200.168.12.17 255.255.255.240
ip nat outside
!
```

```
ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
ip nat inside source list 1 pool net200
!
access-list 1 permit 192.168.12.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that the NAT should be performed on the traffic that passes this interface.
ip nat inside destination	Enables NAT for the inside destination address.
ip nat outside source	Enable NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

ip nat keepalive

Use this command to send ARP requests destined for the addresses in the NAT address pool periodically to verify that the addresses exist.

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

ip nat keepalive *interval-num*

no ip nat keepalive

Parameter Description

Parameter	Description
interval-num	Sets the interval at which ARP packets are sent.

Defaults ARP request packet is not sent by default.

Command Mode Global configuration mode.

Usage Guide

Configuration Examples The following example sets the interval at which ARP packets are sent.

```
Ruijie(config)#ip nat keepalive 100
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

ip nat outside source

Use this command to enble enable NAT for the external source address in global configuration mode. Use the **no** form of this command is used to disable NAT for external source addresses.

ip nat outside source list *access-list-number* **pool** *pool-name* [**vrf** vrf_*name*]

no ip nat outside source list *access-list-number* [**vrf** vrf_*name*]

ip nat outside source static *global-ip local-ip* [**vrf** vrf_*name*]

no ip nat outside source static *global-ip local-ip* [**vrf** vrf_*name*]

ip nat outside source static *protocol global-ip global-port local-ip local-port* [**vrf** vrf_*name*]

no ip nat outside source static *protocol global-ip global-port local-ip local-port* [**vrf** vrf_*name*]

Parameter Description

Parameter	Description
list *access-list-number*	Global address access list. NAT entries will be created only for the traffic with the source address that matches this access list.
pool *pool-name*	Uses a local address in the address pool to perform NAT.
static *global-ip local-ip*	Defines the simple static NAT. *local-ip* is a local address, and *global-ip* is a global address.
static *protocol*	Defines the extended static NAT. *protocol* can be either TCP or UDP.
local-port	Service port number (TCP or UDP) of the local address. Each service typically corresponds to a service port. This port number can be different from *global-port*.
global-port	Service port number of the global address
vrf *vrf_name*	VRF name, which is effective in this VRF.

Defaults NAT for external source addresses is not performed by default.

Command Mode Global configuration mode (this command is not supported on the NPE80)

Usage Guide NAT for external source addresses is mainly used for the overlapped address space. Two private networks to be interconnected are assigned with the same IP address, or a private network and a public network are assigned with the same global IP address, which is called address overlap. Two network hosts with the overlapped address cannot communicate with each other because they both determine that the remote host is located in the local network. Overlapped address NAT is configured to resolve the problem of communication between networks with the overlapped address. With overlapped address NAT configured, the external network host address behaves like another network host address in the internal network, and vice versa.

Configuration of overlapped address NAT includes two steps: 1) Configure the internal source address NAT; 2) Configure the external source address NAT. The external source address translation can be configured only when the address of the external network is overlapped with that of the internal network. The external source address translation can be configured as static NAT or dynamic NAT.

Address overlap is inevitable when a non-registered global IP address is assigned to connect to the Internet during internal network construction. Because the internal network generally uses the domain name to access the external network host, routers must support NAT for DNS packets.

Configuration Examples

In the following example, the address of the internal network 92.168.12.0/24 is overlapped with that of the external network. After translation, the internal host can access the host in the network segment 92.168.12.0/24 in the external network through the network address 192.168.12.0/24.

```
interface FastEthernet0/0
ip address 92.168.12.55 255.255.255.0
ip nat inside
!
interface Serial0/1
ip address 92.168.100.1 255.255.255.0
ip nat outside
encapsulation ppp
!
ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
ip nat inside source list  1 pool net200
ip nat outside source list 1 pool net192
access-list 1 permit 92.168.12.0 0.0.0.255
!
ip route 192.168.12.0 255.255.255.0 92.168.100.2
```

Static routing must be configured because routing must be determined first before determining whether to perform NAT for packets from inside to outside.

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed for the traffic that passes this interface.
ip nat inside destination	Enables NAT for internal destination address.
ip nat inside source	Enables NAT for internal source address.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description

N/A

ip nat p2p-rate-limit

Use this command to enable rate limit for the BT traffic transmitted on an interface.

Use the **no** form of this command to disable BT traffic rate limit on the interface.

ip nat p2p-rate-limit { **in** | **out** } *NUM*

no ip nat p2p-rate-limit { **in** | **out** }

Parameter Description

Parameter	Description
in	Enables rate limit for the incoming BT traffic on an interface.
out	Enables rate limit for the outgoing BT traffic on an interface.
num	Bit/s, in the range from 64,000 to 1,000,000,000

Defaults BT traffic rate limit is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is supported only on the NPE80.

Configuration Examples The following example enables BT traffic rate limit.

```
interface GigabitEthernet 0/1
 ip nat p2p-rate-limit in 64000
 ip nat inside
 ip address 10.1.1.1 255.255.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet 0/2
 ip nat p2p-rate-limit in 64000
ip nat inside
ip address 10.2.1.1 255.255.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet 0/3
 ip nat p2p-rate-limit in 64000
 ip nat inside
 ip address 10.3.1.1 255.255.0.0
 duplex auto
 speed auto
!
```

```
interface GigabitEthernet 0/4
ip nat p2p-rate-limit out 192000
ip nat outside
 ip address 220.181.28.52 255.255.255.0
 duplex auto
 speed auto
!
```

Related Commands

Command	Description
Ip nat { **inside** | **outside** }	Enables NAT on an interface.

Platform Description N/A

ip nat pool

Use this command to define an address pool for NAT in global configuration mode.
Use the **no** form of this command to delete the address pool.
ip nat pool *pool-name start-ip end-ip* { **netmask** *netmask* |
prefix-length *prefix-length* } [**type rotary**]
NPE80:
ip nat pool *pool-name* { **netmask** *netmask* | **prefix-length**
prefix-length } [**type rotary**] **[hardware]**
no ip nat pool *pool-name*
Other equipment:
ip nat pool *pool-name* { **netmask** *netmask* | **prefix-length**
prefix-length } [**type rotary**]

Parameter Description

Parameter	Description
pool-name	Name of the NAT address pool
start-ip	Start IP address of the NAT address pool
end-ip	End IP address of the NAT address pool
netmask *netmask*	Net mask of an address in the NAT address pool
prefix-length *prefix-length*	Length of the net mask of an address in the NAT address pool
type	Type of the NAT address pool. **rotary** means round robin. That is, each address has the same probability of being assigned. The type is **rotary** no matter whether **rotary** is set. The **rotary** parameter is introduced in order to keep compatible with the command of Cisco.

Defaults No address pool is defined by default.

Command Mode Global configuration mode

Usage Guide If multiple address blocks must be defined for an address pool, first create an empty address pool, and define the address range.

Configuration Examples The following example creates an address pool named **net192**, with the start address 192.168.12.1, end address 192.168.12.254, and a 24-bit net mask.

```
ip nat pool net192 192.168.12.1 200.168.12.254 prefix-length 24
```

Related Commands

Command	Description
address	Defines the address block range of an address pool.
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed for the traffic that passes this interface.
ip nat inside destination	Enables NAT for inside destination addresses.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
show ip nat statistics	Displays IP NAT statistics.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

ip nat translation

Use this command to configure the NAT application layer gateway, which is enabled by default.

ip nat translation { **dns** | **ftp** | **h323** | **mms** | **pptp** | **rtsp** | **sip** | **tftp** }

no ip nat translation [**dns** | **ftp** | **h323** | **mms** | **pptp** | **rtsp** | **sip** | **tftp**]

Parameter Description

Parameter	Description
dns	DNS protocol
ftp	FTP protocol
H323	H.323 protocol
mms	MMS protocol.
pptp	PPTP protocol.
rtsp	RTSP protocol.
sip	SIP protocol.
tftp	TFTP protocol.

Defaults All application layer gateways for NAT are enabled by default.

Command Mode Global configuration mode

Usage Guide In NAT application, the IP addresses and ports of data packets are changed. However, the IP addresses and ports of certain special protocols are contained in the valid data of the application layer. To successfully perform NAT for such special protocols, the specific protocol gateway needs to be enabled.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip nat statistics

Use this command to show IP NAT statistics.

show ip nat statistics rule [**nouse** | **syn**]

Parameter Description

Parameter	Description
nouse	Displays unmatched NAT rule.
syn	Synchronizes NAT statistics from the line card (Only valid on RSR77 series).

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the output of the **show ip nat statistics rule** command.

```
Ruijie#show ip nat statistics rule
ip nat inside source static 1.1.1.1 2.2.2.2
       used 0 times
ip nat inside source list 1 interface GigabitEthernet 0/0/3
       used 1 times
Ruijie#show ip nat statistics rule nouse
ip nat inside source static 1.1.1.1 2.2.2.2
```

```
ip nat inside source list 1 interface GigabitEthernet 0/0/3
Ruijie#show ip nat statistics rule syn nat read linecard complete!
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip nat translations

Use this command to query NAT entries in privileged EXEC mode.

show ip nat translations [*acl_num* | **gre** | **icmp** | **tcp** | **udp**] [**vrf** *vrf_name*] [**verbose**]

Parameter Description

Parameter	Description
icmp	Displays NAT entries only for ICMP.
tcp	Displays NAT entries only for TCP.
udp	Displays NAT entries only for UDP.
gre	Displays NAT entries only for GRE.
acl_num	ACL number, which supports only the extended ACL to filter the displayed content.
vrf_name	VRF name. The NAT table is filtered and displayed based on the VRF name.
verbose	Displays more detailed NAT entries.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to display the summary of IP NAT entries, such as protocols, internal global addresses and port numbers, internal local addresses and port numbers, external local addresses and port numbers, and external global addresses and port numbers. Used with the **verbose** parameter, it displays more detailed information, including the timeout period configured for each entry, remaining time for this entry, and flag of the entry.

Configuration Examples The following example displays the output of the **show ip nat translations verbose** command.

```
Ruijie# show ip nat translations verbose
timeout for NAT TCP flows: 86400
timeout for NAT TCP flows after a FIN or RST: 60
timeout for NAT TCP flows after a SYN : 60
timeout for NAT UDP flows: 300
```

```
timeout for NAT DNS flows: 60
timeout for NAT ICMP flows: 60
Pro Inside global     Inside local      Outside local     Outside global
timeout vrf
tcp 192.168.5.103:1987 192.168.211.21:1987 211.67.71.7:80    211.67.71.7:80
timeout=85139 1
udp      192.168.5.103:1041     192.168.211.183:1041     202.101.98.55:53
202.101.98.55:53 timeout=38 1
```

The meanings of the various fields in the output are as follows:

Field	Description
Pro	Protocol type. **udp** indicates the UDP translation entry. **tcp** indicates the TCP translation entry. **icmp** indicates the ICMP translation entry.
Inside global	Internal global address and port number
Inside local	Internal local address and port number
Outside local	External local address and port number
Outside global	External global address and port number
timeout	Time (in seconds) left before this NAT entry times out
vrf	VRF where the connection is

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Performs NAT on the traffic that passes this interface.
ip nat inside destination	Enables NAT for internal destination addresses.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description

N/A

AAA Commands

aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure an 802.1x user authentication method list in global configuration mode.
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 of user authentication.
list-name	Specifies the name of an 802.1x user authentication method list, which can 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	Authentication is not performed.
group	Uses a server group for authentication. Currently, 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 equipment, AAA is required for 802.1x user authentication negotiation. Use the **aaa authentication dot1x** command to configure a default or an optional method list of 802.1x user authentication.
The next method can be used for authentication only when the current method does not respond.

Configuration Examples The following example defines an AAA 802.1x user authentication method list named **rds_d1x**. In the authentication method list, the RADIUS security server is used for authentication first. If the RADIUS security server does not respond within the specified period of time, 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

aaa authentication enable

Use this command to enable AAA Enable authentication and configure an Enable authentication method list in global configuration mode.

Use the **no** form of this command to delete the user authentication method list.

aaa authentication enable default *method1* [*method2*...]

no aaa authentication enable default

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method of Enable authentication. Enable authentication is global authentication. Currently, only configuration of a default authentication method list is supported.
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	Authentication is not performed.
group	Uses a server group for authentication. Currently, 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 equipment, AAA is required for Enable authentication negotiation. Use the **aaa authentication enable** command to configure a default method list of Enable authentication.

The next method can be used for authentication only when the current method does not respond.

The Enable authentication function automatically takes effect after the Enable authentication method list is configured.

Configuration Examples The following example defines an AAA Enable authentication method list. In the authentication method list, the RADIUS security server is used for authentication first. If the RADIUS security server does not respond with the specified period of time, 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	Switches the user level.
username	Defines a local user database.

Platform Description N/A

aaa authentication login

Use this command to enable AAA login authentication and configure a login authentication method list in global configuration mode.

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 of login authentication.
list-name	Specifies the name of a login authentication method list, which can be any character strings.
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	Identify authentication is not performed.
group	Uses a server group for authentication. Currently, 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 equipment, AAA is required for login authentication negotiation. Use the **aaa authentication login** command to configure a default or an optional method list of login authentication.

The next method can be used for authentication only when the current method does not respond.

You must apply the configured login authentication method to the terminal line that requires login authentication; otherwise, the configured login authentication method is ineffective.

Configuration Examples The following example defines an AAA login authentication method list named **list-1**. In the authentication method list, the RADIUS security server is used for authentication first. If the RADIUS security server does not respond within the specified period of time, 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.
username	Defines a local user database.
login authentication	Applies the login authentication method to a terminal line.

Platform Description N/A

aaa authentication ppp

Use this command to enable AAA PPP user authentication and configure a PPP user authentication method list in global configuration mode.

Use the **no** form of this command to delete the authentication method list.

aaa authentication ppp { **default** | *list-name* } *method1* [*method2*...]

no aaa authentication ppp { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method of PPP user authentication.
list-name	Specifies the name of a PPP user authentication method list, which can be any character strings.
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	Identity authentication is not performed.
group	Uses a server group for authentication. Currently, the RADIUS and TACACS+ server groups are supported.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If the AAA PPP security service is enabled on equipment, AAA is required for PPP authentication negotiation. Use the **aaa authentication ppp** command to configure a default or an optional method list of PPP user authentication.

The next method can be used for authentication only when the current method does not respond.

Configuration Examples The following example defines an AAA PPP authentication method list named **rds_ppp**. In the authentication method list, the RADIUS security server is used for authentication first. If the RADIUS security server does not respond within the specified period of time, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication ppp rds_ppp group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
ppp authentication	Associates a specific method list with a PPP user.
username	Defines a local user database.

Platform Description N/A

login authentication

Use this command to apply a login authentication method list to the specified terminal line.

Use the **no** form of this command to remove the application of the login authentication method list.

login authentication {default | *list-name*}

no login authentication

Parameter Description

Parameter	Description
default	Applies the default login authentication method list.
list-name	Applies a defined login authentication method list.

Defaults N/A

Command Mode Line configuration mode

Usage Guide Once the default login authentication method list has been configured, it will be applied to all terminals automatically. If a non-default login authentication method list has been applied to a terminal, it will replace the default one. If you attempt to apply an undefined method list, you will be notified that the login authentication on this line is ineffective until the method list is defined.

Configuration Examples The following example defines an AAA login authentication method list named **list-1**. In the authentication method list, the local user database is used for authentication first. Then, apply this method to VTY 0-4.

```
Ruijie(config)# aaa authentication login list-1 local
Ruijie(config)# line vty 0 4
Ruijie(config-line)# login authentication list-1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
username	Defines a local user database.
login authentication	Configures a login authentication method list.

Platform Description N/A

aaa authorization commands

Use this command to authorize the commands executed by users that have logged in to the network access server (NAS) command-line interface (CLI).

Use the **no** form of this command to disable the AAA command authorization function.

aaa authorization commands *level* {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization commands *level* {**default** | *list-name*}

Parameter Description

Parameter	Description
level	Specifies the command level to be authorized, in the range from 0 to 15. You can run this command after the authorization of a specific command level is passed.
default	When this parameter is used, the following defined method list is used as the default method of command authorization.
list-name	Specifies the name of a command authorization method list, which can be any character strings.
method	It must be one of the keywords: **local**, **none**, **and group**. One method list can contain up to four methods.
none	Authorization is not performed.
group	Uses a server group for authorization. Currently, the TACACS+ server group is supported

Defaults AAA command authorization is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS supports authorization of the commands executed by users. When a user inputs and attempts to run a command, AAA sends this command to the security server. This command will be executed if the security server allows command execution; otherwise, it will prompt command execution denial.

You are required to specify the command level when configuring command authorization. This specified command level is the default command level (for example, the default level of a command is 14 when the command is visible for users above level 14).

You must apply the configured command authorization method to the terminal line that requires command authorization; otherwise, the configured command authorization method is ineffective.

Configuration Examples The following example uses the TACACS+ server to authorize level 15 commands.

```
Ruijie(config)# aaa authorization commands 15 default group tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Applies command authorization to a terminal line.

Platform Description N/A

aaa authorization config-commands

Use this command to authorize configuration commands (including in global configuration mode and its sub-mode) through AAA.

Use the **no** form of this command to disable the AAA authorization function for configuration commands.

aaa authorization config-commands

no aaa authorization config-commands

Parameter Description

Parameter	Description
N/A	N/A

Defaults Configruation command authorization is disabled by default.

Command Mode Global configuration mode

Usage Guide If you only need to authorize commands in non-configuration mode (for example, in privileged EXEC mode), use the no form of this command to disable the authorization function in configuration mode. This action allows you to run commands in 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 AAA command authorization.

Platform Description N/A

aaa authorization console

Use this command to authorize the commands executed by users that log in from the console in global configuration mode.

Use the **no** form of this command to disable the AAA command authorization function.

aaa authorization console

no aaa authorization console

Parameter Description

Parameter	Description
N/A	N/A

Defaults Command authorization for users on the console is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS supports identifying users that log in from the console and from other terminals. You can configure whether to authorize the commands executed by users that log in from the console. If the command authorization function is disabled on the console, the command authorization method list applied to the console line is ineffective.

Configuration Examples The following example enables the command authorization function for users that log in from the console.

```
Ruijie(config)# aaa authorization console
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Defines AAA command authorization.
authorization commands	Applies command authorization to a terminal line.

Platform Description N/A

aaa authorization exec

Use this command to perform AAA EXEC authorization on users that have logged in to the NAS CLI and assign authority levels.

Use the **no** form of this command to disable the AAA EXEC authorization function.

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 of EXEC authorization.
list-name	Specifies the name of an EXEC authorization method list, which can be any character strings.
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 authorization.
none	Authorization is not performed.
group	Uses a server group for authorization. Currently, the RADIUS and TACACS+ server groups are supported.

Defaults AAA EXEC authorization is disabled by default.

Command Global configuration mode

Mode

Usage Guide RGOS supports authorization of users that have logged in to the NAS CLI and assignment of CLI authority levels (in the range from 0 to 15). The EXEC authorization function is effective only for users that pass login authentication. Users cannot enter the CLI if EXEC authorization fails.
You must apply the configured EXEC authorization method to the terminal line that requires EXEC authorization; otherwise the configured method is ineffective.

Configuration Examples The following example uses the RADIUS server to implement EXEC authorization.

```
Ruijie(config)# aaa authorization exec default group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
authorization exec	Applies authorization to a terminal line.
username	Defines a local user database.

Platform Description N/A

aaa authorization network

Use this command to perform AAA authorization on the service requests (including such protocols as PPP and SLIP) from users that access networks in global configuration mode.
Use the **no** form of this command to disable the AAA authorization function.
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 of network authorization.
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Network authorization is not performed.
group	Uses a server group for authorization. Currently, the RADIUS and TACACS+ server groups are supported.

Defaults AAA network authorization is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS supports authorization of all network-related service requests, such as PPP and SLIP. If

authorization is configured, all authenticated users or interfaces will be authorized automatically.
Three different authorization methods can be specified. Like identity authentication, the next method can be used for authorization only when the current authorization method does not respond. If the current authorization method fails, the subsequent authorization method is not used.
The RADIUS or TACACS+ server authorizes authenticated users by returning a series of attributes. Therefore, network authorization is based on autheitcation. Network authorization is performed only on authenticated users.

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 identity authentication.
username	Defines a local user database.

Platform Description N/A

authorization commands

Use this command to apply a command authorization method list to the specified terminal line in line configuration mode.
Use the **no** form of this command to remove the application of the command authentication method list.
authorization commands *level* { **default** | *list-name* }
no authorization commands *level*

Parameter Description

Parameter	Description
level	Specifies the command level to be authorized, in the range from 0 to 15. You can run this command after the authorization of a specific command level is passed
default	When this parameter is used, the following defined method list is used as the default method of command authorization.
list-name	Applies a defined command authorization method list.

Defaults AAA command authorization is disabled by default.

Command Mode Line configuration mode

Usage Guide Once the default command authorization method list has been configured, it will be applied to all terminals automatically. If a non-default command authorization method list is applied to a terminal, it

will replace the default one. If you attempt to apply an undefined method list, you will be notified that the command authorization on this line is ineffective until the method list is defined.

Configuration Examples The following example defines a command authorization method list named **cmd** to authorize level 15 commands, and uses TACACS+ as the security server. The none method will be used if the server does not respond. The configured method list is applied to the VTY 0 – 4 line.

```
Ruijie(config)# aaa authorization commands 15 cmd group tacacs+ none
Ruijie(config)# line vty 0 4
Ruijie(config-line)# authorization commands 15 cmd
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
authorization commands	Applies the AAA command authorization method list.

Platform Description N/A

authorization exec

Use this command to apply an EXEC authorization method list to the specified terminal line.
Use the **no** form of this command to remove the application of the EXEC authentication method list.
authorization exec { **default** | *list-name* }
no authorization exec

Parameter Description

Parameter	Description
default	Applies the default EXEC authorization method.
list-name	Applies a defined EXEC authorization method list.

Defaults No default AAA EXEC authentication method list is configured.

Command Mode Line configuration mode.

Usage Guide Once the default EXEC authorization method list has been configured, it will be applied to all terminals automatically. If a non-default EXEC authorization method list is applied to a line, it will replace the default one. If you attempt to apply an undefined method list, you will be notified that the EXEC authorization on this line is ineffective until the method list is defined.

Configuration Examples The following example defines an EXEC authorization method list named **exec-1**, and uses RADIUS as the security server. The none method will be used if the server does not respond. The configured method list is applied to the VTY 0 – 4 line.

```
Ruijie(config)# aaa authorization exec exec-1 group radius none
Ruijie(config)# line vty 0 4
Ruijie(config-line)# authorization exec exec-1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Defines an AAA EXEC authorization method list.

Platform Description N/A

aaa accounting commands

Use this command to perform accounting on the command activities of users that have logged in to the NAS in global configuration mode in order to manage user activities.

Use the **no** form of this command to disable the command accounting function.

aaa accounting commands *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]

no aaa accounting commands *level* { **default** | *list-name* }

Parameter Description

Parameter	Description
level	Specifies the command level for accounting, in the range from 0 to 15. Related messages are recorded when you determine which command level is executed.
default	When this parameter is used, the following defined method list is used as the default method of command accounting.
list-name	Speficies the name of a command accounting method list, which can 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	Accounting is not performed.
group	Uses a server group for accounting. Currently, the TACACS+ server group is supported.

Defaults Accounting is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS enables the command accounting function only after users pass login authentication. Command accounting is not performed when users are not anthenticated upon login or the none authentication method is used. After the accounting function is enabled, command information is sent to the security service each time when users run the specified level of commands.

You must apply the configured command accounting method to the terminal line that requires command accounting; otherwise, the configured command accounting method is ineffective.

Configuration Examples The following example performs accounting on the command requests from usersby using TACACS+, and configures 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 identity authentication.
accounting commands	Applies command accounting to a terminal line.

Platform Description N/A

aaa accounting exec

Use this command to perform accounting on the access activities of users that log in to the NAS in global configuration mode in order to manage user activities.

Use the **no** form of this command to disable the EXEC accounting function.

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 of EXEC accounting.
list-name	Specifies the name of an EXEC accounting method list, which can 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	Accounting is not performed.
group	Uses a server group for accounting. Currently, the RADIUS and TACACS+ server groups are supported.

Defaults Accounting is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS enables the EXEC accounting function only after users pass login authentication. EXEC accounting is not performed when users are not anthenticated upon login or the none authentication method is used.

After the accounting function is enabled, an accounting start message is sent to the security server when a user logs in to the NAS CLI, and an accounting stop message is sent to the security server when the user logs out. If an accounting start message is not sent to the security server when a user logs in, an accounting stop message is not sent to the security server when the user logs out.

You must apply the configured EXEC accounting method to the terminal line that requires command accounting; otherwise, the configured EXEC accounting method is ineffective..

Configuration The following example performs accounting on users' NAS login activities by using RADIUS, and

Examples sends accounting messages at the start time and end time of access.

```
Ruijie(config)# aaa accounting exec default start-stop group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication	Defines AAA identity authentication.
accounting commands	Applies EXEC accounting to a terminal line.

Platform Description N/A

aaa accounting network

Use this command to perform accounting on users' access activities in global configuration mode in order to count network access fees or manage user activities.

Use the **no** form of this command to disable the network accounting function.

aaa accounting network {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting 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 of network accounting.
list-name	Specifies the name of an accounting method list.
start-stop	Sends accounting messages at both the start time and end time of users' network access. Users are allowed to access networks regardless of whether the accounting start message enables accounting successfully.
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Accounting is not performed.
group	Uses a server group for accounting. Currently, the RADIUS and TACACS+ server groups are supported.

Defaults Accounting is disabled by default.

Command Mode Global configuration mode

Usage Guide RGOS performs accounting on 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 on the network service requests from users by using RADIUS, and sends accounting messages at the start time and end time of network access:

```
Ruijie(config)# aaa accounting network default start-stop group radius
```

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization network	Defines AAA network authorization.
	aaa authentication	Defines AAA identity authentication.
	username	Defines a local user database.

Platform Description N/A

aaa accounting update

Use this command to enable the accounting update function in global configuration mode.
Use the **no** form of this command to disable the accounting update function.
aaa accounting update
no aaa accounting update

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Accounting update 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 update function after the AAA security service is enabled.

Configuration Examples The following example enables the accounting update function.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting updatee
```

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

aaa accounting update periodic

Use this command to set the accounting update interval in global confguration mode after the accounting update function is enabled.
Use the **no** form of this command to restore the accounting update interval to the default value.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter Description

Parameter	Description
interval	Specifies the accounting update interval, in minutes. The shortest interval is one minute.

Defaults The default accounting update interval is five minutes.

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 update interval after the AAA security service is enabled.

Configuration Examples The following example sets the accounting update interval to one 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

accounting commands

Use this command to apply a command accounting list to the specified terminal line in line configruation mode.

Use the **no** form of this command to disable the command accounting function on the terminal line.

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

no accounting commands *level*

Parameter Description

Parameter	Description
level	Specifies the command level for accounting, in the range from 0 to 15.
default	Applies the default command accounting method.
list-name	Uses a defined command accounting method list.

Defaults Accounting is disabled by default.

Command Mode Line configuration mode

Usage Guide Once the default command accounting method list has been configured, it will be applied to all terminals automatically. If a non-default command accounting method list has been applied to a line, it will replace the default one. If you attempt to apply an undefined method list, you will be notified that the command accounting on this line is ineffective until the method list is defined.

Configuration Examples The following example defines a command accounting method list named **cmd** to authorize level 15 commands, and uses TACACS+ as the security server. The none method will be used if the server does not respond. The configured method list is applied to the VTY 0 – 4 line.

```
Ruijie(config)# aaa accounting commands 15 cmd group tacacs+ none
Ruijie(config)# line vty 0 4
Ruijie(config-line)# accounting commands 15 cmd
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accouting commands	Defines an AAA command accounting method list.

Platform Description N/A

accounting exec

Use this command to apply an EXEC accouting method list to the specified terminal line in line configuration mode.
Use the **no** form of this command to disable the EXEC accounting function on the terminal line.
accounting exec {**default** | *list-name*}
no accounting exec

Parameter Description

Parameter	Description
default	Applies the default EXEC accounting method.
list-name	Uses a defined EXEC accounting method list.

Default Accounting is disabled by defaults.

Command Mode Line configuration mode

Usage Guide Once the default EXEC accounting method list has been configured, it will be applied to all terminals automatically. If a non-default EXEC accounting method list has been applied to a line, it will replace the default one. If you attempt to apply an undefined method list, you will be notified that the EXEC accounting on this line is ineffective until the method list is defined.

Configuration Examples The following example defines an EXEC accounting method list named exec-1, and uses RADIUS as the security server. The none method will be used if the server does not respond. The configured

method list is applied to the VTY 0 – 4 line.

```
Ruijie(config)# aaa accounting exec exec-1 group radius none
Ruijie(config)# line vty 0 4
Ruijie(config-line)# accounting exec exec-1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accouting commands	Defines an AAA EXEC accouting method list.

Platform Description N/A

aaa domain

Use this command to enter domain configuation mode and configure domain attributes.

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

aaa domain {**default** | *domain-name*}

no aaa domain {**default** | *domain-name* }

Parameter Description

Parameter	Description
default	Configures the default domain.
domain-name	Specifies the name of a 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** parameter is used to configure the default domain. That is the method list used by network equipment if users do not carry domain information. The *domain-name* parameter is used to configure the specified domain name. If users carry this domain name, the method lists associated with this domain are used. Currently, the system can configure up to 32 domains.

Configuration Examples The following example configures a 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 domain configuration.

Platform N/A

Description

aaa doman enable

Use this command to enable the domain name-based AAA service, which is disabled by default. When the domain name-based AAA service is enabled, the domain name-based AAA service configuration is preferred.

Use the **no** form of this command to disable the domain name-based AAA service.

aaa domain enable

no aaa domain enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The domain name-based AAA service is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the domain name-based AAA service when you perform domain name-based AAA service configuration.

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 domain configuration.

Platform Description N/A

access-limit

Use this command to configure the maximum number of users for domains, which is valid only for IEEE802.1x users.

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

access-limit *num*

no access-limit

Parameter Description

Parameter	Description
num	Maximum number of users for domains, which is valid only for IEEE802.1x users

Defaults The number of users is not limited by default.

Command Mode Domain configuration mode

Usage Guide Use this command to configure the maximum number of users for domains.

Configuration Examples The following example sets the maximum number of users to 20 for the domain named **ruijie.com**.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# access-limit 20
```

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 domain configuration.

Platform Description N/A

accounting network

Use this command to configure a network accounting method list in domain conifguration mode.
Use the **no** form of this command to remove the setting.
accounting network { **default** | *list-name* }
no accounting network

Parameter Description

Parameter	Description
default	Specifies the default method list.
list-name	Specifies the name of a method list.

Defaults With no method list specified, if a user sends a request, network equipment will attempt to specify the default method list for the user.

Command Mode Domain configuration mode

Usage Guide Use this command to configure a network accounting method list for a domain.

Configuration Examples The following example configures a network accounting method list for a 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 domain configuration.

Platform Description N/A

authentication dot1x

Use this command to configure an IEEE802.1x authentication method list in domain configuration mode.

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

authentication dot1x { **default** | *list-name* }

no authentication dot1x

Parameter Description

Parameter	Description
default	Specifies the default method list.
list-name	Specifies the name of a method list.

Defaults With no method list specified, if a user sends a request, network equipment will attempt to specify the default method list for the user.

Command Mode Domain configuration mode

Usage Guide Use this command to configure an IEEE802.1x authentication method list for a domain.

Configuration Examples The following example configures an IEEE802.1x authentication method list for a 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 domain configuration.

Platform Description N/A

authorization network

Use this command to configure a network authorization list in domain configuration mode.

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

authorization network { **default** | *list-name* }

no authorization network

Parameter Description

Parameter	Description
default	Specifies the default method list.
list-name	Specifies the name of a method list.

Defaults With no method list specified, if a user sends a request, network equipment will attempt to specify the default method list for the user.

Command Mode Domain configuration mode

Usage Guide Use this command to configure a network authorization list for a domain.

Configuration Examples The following example configures a network authorization list for a 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 domain configuration.

Platform Description N/A

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 configured domain is valid by default.

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 domain configuration .

Platform Description N/A

show aaa domain

Use this command to query all current domain information

show aaa domain [**default** | *domain-name*]

Parameter Description

Parameter	Description
default	Displays the default domain information.
domain-name	Displays information about the specified domain.

Defaults N/A

Command Mode Privileged EXEC 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# 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

username-format

Use this command to configure whether user names carry domain information when the NAS interacts with servers.

Use the **no** form of this command restores to the default setting.

username-format { **without-domain** | **with-domain** }

no username-format

Parameter Description

Parameter	Description
without-domain	Domain information is removed from user names.
with-domain	Domain information is retained in user names.

Defaults Domain information is retained in user names by default.

Command Mode Domain configuration mode

Usage Guide Use this command to configure whether user names carry domain information when the NAS interacts with servers.

Configuration Examples The following example configures a user name to remove 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 domain configuration.

Platform Description N/A

aaa group server

Use this command to enter AAA server group comfiguration mode.

Use the **no** form of this command to delete server groups.

aaa group server { **radius** | **tacacs+** } *name*

no aaa group server { **radius** | **tacacs+** } *name*

Parameter Description

Parameter	Description
name	Name of a server group. It cannot be the keywords **radius** or **tacacs+**

	because RADIUS and TACACS+ are the default server group names.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to confgure AAA server groups. Currently, the RADIUS and TACACS+ server groups are supported.

Configuration Examples The following example configures an AAA server group.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Group Name:  ss
Group Type:  radius
Referred:    1
Server List:
```

Related Commands

Command	Description
show aaa group	Displays AAA server group information.

Platform Description N/A

ip vrf forwarding

Use this command to select VPN routing and forwarding (VRF) for an AAA server group.
Use the **no** form of this command to remove the setting.
ip vrf forwarding *vrf_name*
no ip vrf forwarding

Parameter Description

Parameter	Description
vrf_name	VRF name

Defaults N/A

Command Mode Server group configuration mode

Usage Guide Use this command to select VRF for the specified server group.

Configuration Examples The following example selects VRF for a server group.

```
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
aaa group server	Configures an AAA server group.
show aaa group	Displays AAA server group information.

Platform Description N/A

server

Use this command to add a server to an AAA server group.

Use the **no** form to delete a server.

server *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]

no server *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]

Parameter Description

Parameter	Description
ip-addr	IP address of a server
port1	Authentication port of a server (which is supported only by the RADIUS server group)
port2	Accounting port of a server (which is supported only by the RADIUS server group)

Defaults No server is configured by default.

Command Mode Server group configuration mode

Usage Guide Use this command to add a server to the specified server group. The default value is used if no port is specified.

Configuration Examples

The following example adds a server to a server group.

```
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
Ruijie# show aaa group
Type      Reference  Name
---------- ---------- ----------
radius    1         radius
tacacs+   1         tacacs+
radius    1         ss
```

Related

Command	Description

Commands		
	aaa group server	Configures an AAA server group.
	show aaa group	Displays AAA server group information.

Platform Description N/A

show aaa group

Use this command to query 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

Usage Guide Use this command to query all the server groups configured for AAA.

Configuration Examples

The following example displays all the server groups configured for AAA.

```
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 an AAA server group.

Platform Description N/A

aaa local authentication attempts

Use this command to configure the maximum number of login attempt times.

aaa local authentication attempts *max-attempts*

Parameter Description	Parameter	Description
	max-attempts	Maximum number of login attempt times, in the range from 1 to 2147483647

Defaults The default value is 3.

Command Mode Global configuration mode

Usage Guide Use this command to configure the maximum login attempt times.
The following example sets the maximum login attempt times to 6.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# aaa local authentication attempts 6
```

Related Commands

Command	Description
show running-config	Displays the current equipment configuration.
show aaa lockout	Displays the lockout configuration parameter of the current login.

Platform Description N/A

aaa local authentication lockout-time

Use this command to configure the length of lockout-time when the maximum login attempt times are exceeded.
aaa local authentication lockout-time *lockout-time*

Parameter Description

Parameter	Description
lockout-time	Length of lockout-time, in the range from 1 to 2147483647.

Defaults 15 hours.

Command Mode Global configuration mode

Usage Guide Use this command to configure the length of lockout-time when the maximum login attempt times are exceeded.
The following example sets the length of lockout-time to 5 hours.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# aaa local authentication lockout-time 5
```

Related Commands

Command	Description
show running-config	Displays the current equipment configuration.
show aaa lockout	Displays the lockout configuration parameter of the current login.

Platform Description N/A

aaa new-model

Use this command to enable the RGOS AAA security service in global configuration mode.
Use the **no** form of this command to disable the AAA security service.
aaa new-model
no aaa new-model

Parameter Description

Parameter	Description
N/A	N/A

Defaults The AAA security service 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

clear aaa local user lockout

Use this command to clear a lockout user list.
clear aaa local user lockout { **all** | **user-name** <*word*> }

Parameter Description

Parameter	Description
<*word*>	User ID

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear all lockout user lists or the specified lockout user list.

Configuration Examples The following example clears all lockout user lists

```
Ruijie# clear aaa local user lockout all
```

Related Commands

Command	Description
show running-config	Displays the current equipment configuration.
show aaa lockout	Displays the lockout configuration parameter of the current login.

Platform Description N/A

debug aaa

Use this command to enable the AAA service debugging switch.

Use the **no** form of this command to disable the debugging switch.

debug aaa event

no debug aaa event

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

show aaa method-list

Use this command to query all AAA method lists.

show aaa method-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query all AAA method lists.

Configuration Examples

The following example displays AAA method lists.

```
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

show aaa user lockout

Use this command to query the current lockout user list.

show aaa user lockout

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the current lockout user list and the length of lockout-time.

Configuration Examples The following example displays the current lockout user list.

```
Ruijie# show aaa user lockout
```

Related Commands

Command	Description
show running-config	Displays the current equipment configuration.
show aaa lockout	Displays the lockout configuration parameter of the current login.

Platform Description N/A

RADIUS Commands

ip radius source-interface

Use this command to specify the source IP address of the RADIUS packet in global configuration mode.
Use the **no** form of this command to delete the source IP address of the RADIUS packet.
ip radius source-interface *interface*

no radius source-interface

Parameter Description

Parameter	Description
Interface	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 by default.

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 on 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 an interface.

Platform Description N/A

radius attribute

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

Defaults

Only the default configuration of private attributes in Ruijie is recognized.

id	Function	Type
1	max down-rate	1
2	qos	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
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	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dialup-avoid	21
22	ip privilege	22
23	login privilege	42

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	dialup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Command Mode Global configuration mode

Usage Guide Use this command to configure the type value of a private attribute.

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

radius-server attribute 31

Use this command to specify the MAC-based format of the RADIUS Calling-Station-ID attribute in global configuration mode.

Use the **no** form of this command to restore the default value.

radius-server attribute 31 mac format { **ietf** | **normal** | **unformatted** }

no radius-server attribute 31 mac format

Parameter Description

Parameter	Description
ietf	Standard format specified by the IETF (RFC3580). The hyphen (-) is used as the separator, for example: 00-D0-F8-33-22-AC.
normal	Normal format representing the MAC address. The hyphen (-) is used as the separator. For example: 00d0.f833.22ac.
unformatted	No format and separator, which is used by default, for

	example: 00d0f83322ac

Defaults The default format is unformatted.

Command Mode Global configuration mode

Usage Guide Some RADIUS security servers (mainly used in 802.1x authentication) may identify only the IETF format. In this case, the RADIUS Calling-Station-ID attribute must be set to the IETF format type.

Configuration Examples The following example defines the RADIUS Calling-Station-ID attribute as the IETF format.

```
Ruijie(config)# radius-server attribute 31 mac format ietf
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

radius-server dead-ctriteria

Use this command to configure criteria on a device to determine that the RADIUS security server is unreachable in global configuration mode.
Use the **no** form of this command to restore the default value.
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 period. If a device does not receive a correct response packet from the RADIUS security server within the specified time, the RADIUS security server is considered to be unreachable. The value ranges from 1s to 120s.
tries *number*	Configures the successive timeout times. When sending a request from a device to the same RADIUS security server times out for the specified times successively, the device considers the RADIUS security server to be unreachable. The value ranges from 1 to 100.

Defaults **time** *seconds*: 60s
tries *number*: 10

Command Mode Global configuration mode

Usage Guide If a RADIUS security server meets the timeout period and successive timeout times at the same time, the device considers the RADIUS security server to be unreachable. You can use this command to adjust the parameters of the timeout period and successive timeout times.

Configuration Examples The following example sets the timeout period to 120s and the successive timeout times to 20.

```
Ruijie(config)# radius-server dead-criteria time 120 tries 20
```

Related commands

Command	Description
radius-server host	Defines the host of the RADIUS security server.
radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable RADIUS security server.
radius-server timeout	Defines the timeout period of RADIUS packet retransmission.

Platform Description N/A

radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable RADIUS security server in global configuration mode.
Use the **no** form of this command to return to the default value.
radius-server deadtime *minnutes*
no radius-server deadtime

Parameter Description

Parameter	Description
minutes	Defines the duration (in minutes) when a device stops sending any requests to the unreachable RADIUS security server. The value ranges from 1 minute to 1440 minute (24 hours).

Defaults The default value of the minutes parameter is 0 minutes. That is, a device keeps sending requests to the unreachable RADIUS security server.

Command Mode Global configuration mode

Usage Guide If active RADIUS server detection is enabled on a device, the minutes 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 a device stops sending requests to a RADIUS server to 1 minute.

```
Ruijie(config)# radius-server deadtime 1
```

Related Commands	Command	Description
	radius-server dead-criteria	Defines the criteria of determining that a RADIUS server is unreachable.
	radius-server host	Defines host information of the RADIUS security server.

Platform Description N/A

radius-server host

Use this command to specify a RADIUS security server host in global configuration mode.

Use the **no** form of this command to delete the RADIUS security server host.

radius-server host { *ipv4-address* | *ipv6-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]]

no radius-server host { *ipv4-address* | *ipv6-address*}

Parameter Description

Parameter	Description
ipv4-address	IPv4 address of the RADIUS security server host
ipv6-address	IPv6 address of the RADIUS security server host
auth-port	UDP port for RADIUS authentication
*port-numbe*r	Number of the UDP port used for RADIUS authentication. If it is set to 0, the host does not perform authentication.
acct-port	UDP port for RADIUS accounting
port-number	Number of the UDP port for RADIUS accounting. If it is set to 0, the host does not perform accounting.
test username *name*	(Optional) Enables active detection of the RADIUS security server and specifies the user name used by active detection.
idle-time *time*	(Optional) Sets the interval of sending test packets to the reachable RADIUS security server, which is 60 minutes by default and in minute the range from 1 to 1440 minutes (namely 24 hours).
ignore-auth-port	(Optional) Disables detection of the authentication port on the RADIUS security server. It is enabled by default.
ignore-acct-port	(Optional) Disables detection of the accounting port on the RADIUS security server. It is enabled by default.

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 by using this command.

Configuration The following example defines an IPv4 RADIUS security server host.

Examples

```
Ruijie(config)# radius-server host 192.168.12.1
```

The following example defines an IPv4 RADIUS security server host, enables active detection with the detection interval 60 minutes, and disables 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 an IPv6 RADIUS security server host.

```
Ruijie(config)# radius-server host 3000::100
```

Related Commands

Command	Description
aaa authentication	Defines the AAA identity authentication method list.
radius-server key	Defines a shared password for the RADIUS security server.
radius-server retransmit	Define the RADIUS packet retransmission times.
radius-server timeout	Defines the timeout period of RADIUS packet retransmission.
radius-server dead-criteria	Defines the criteria of determining that a RADIUS server is unreachable.
radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable RADIUS security server.

Platform Description

N/A

radius-server key

Use this command to define a shared password for the network access server (a router) to communicate with the RADIUS security server.

Use the **no** form of this command to remove the shared password.

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: simple encryption

Defaults

No shared password is specified by default.

Command Mode

Global configuration mode

Usage Guide A shared password is the basis for communication between a device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, 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 host.
radius-server retransmit	Defines the RADIUS packet retransmission times.
radius-server timeout	Defines the timeout period of RADIUS packet retransmission.

Platform Description N/A

radius-server retransmit

Use this command to configure the packet retransmission times before a device determines that the RADIUS security server fails to 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	Retransmission times

Defaults The default retransmission times are 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 a device retransmits the RADIUS packet for the specified times and the interval between every two retries times out, the device considers that the security sever fails to respond.

Configuration Examples The following example sets the retransmission times to 4.

```
Ruijie(config)# radius-server retransmit 4
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server host.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Defines the timeout period of RADIUS packet retransmission.

Platform Description N/A

radius-server timeout

Use this command to set the time for a device to wait for a response from the security server before 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 period in the range from 1 second to1000 seconds

Defaults The default timeout period is five seconds.

Command Mode Global configuration mode

Usage Guide Use this command to change the timeout period of packet retransmission.

Configuration Examples The following example sets the timeout period to 10 seconds.

```
Ruijie(config)# radius-server timeout 10
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server host.
radius-server retransmit	Defines the RADIUS packet retransmission times.
radius-server key	Defines a shared password for the RADIUS server.

Platform Description N/A

radius set qos cos

Use this command to set the qos value sent by the RADIUS server as the cos value of an interface.
radius set qos cos
no radius set qos cos

Parameter Description

Parameter	Description
N/A	N/A

Defaults The qos value sent by the RADIUS server is set to the dscp value by default.

Command Mode Global configuration mode

Usage Guide Use this command to set the qos value sent by the RADIUS server to the cos value. The qos value sent by the RADIUS server is set to the dscp value by default.

Configuration Examples The following example sets the qos value sent by the RADIUS server to the cos value of an interface.

```
Ruijie(config)# radius set qos cos
```

Related Commands

Command	Description
radius vendor-specific extend	RADIUS is extended not to differentiate the IDs of private vendors.

Platform Description N/A

radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors.**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 by default.

Command Mode Global configuration mode

Usage Guide Use this command to identify the attributes of all vendor IDs by type.

Configuration Examples The following example extends RADIUS not to differentiate the IDs of private vendors.

```
Ruijie(config)# radius vendor-specific extend
```

Related Commands

Command	Description
radius attribute	Configures the private vendor type.
radius set qos cos	Configures whether the qos value sent by the RADIUS server to the cos value of an interface.

Platform Description N/A

debug radius

Use this command to turn on the RADIUS debugging switch.

Use the **no** form of this command to turn off the RADIUS debugging switch.

debug radius { **event** | **detail** }

no debug radius { **event** | **detail** }

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

show radius parameter

Use this command to query the global parameters of the RADIUS server.

show radius parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A.

Command Privileged EXEC mode

Mode

Usage Guide Use this command to query the global parameters of the RADIUS server.

Configuration Examples

```
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
radius-server host	Defines the RADIUS security server host.
radius-server retransmit	Defines the RADIUS packet retransmission times.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the timeout period of RADIUS packet retransmission
radius-server dead-criteria	Defines the criteria of determining that a RADIUS server is unreachable.
radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable RADIUS security server.

Platform Description N/A

show radius server

Use this command to query the configuration of the RADIUS server.

show radius server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the configuration of the RADIUS server.

Configurati

```
Ruijie# show radius server
```

on

Examples

```
Server IP:  192.168.4.12
Accounting Port: 23
Authen Port:   77
Test Username:  viven
Test Idle Time:  10 Minutes
Test Ports:    Authen
Server State:   Active
  Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP:  192.168.4.13
Accounting Port: 45
Authen Port:   74
Test Username:  <Not Configured>
Test Idle Time:  60 Minutes
Test Ports:    Authen and Accounting
Server State:   Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server host.
radius-server retransmit	Defines the RADIUS packet retransmission times.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the timeout period of RADIUS packet retransmission.

Platform Description

N/A

show radius vendor-specific

Use this command to query the configuration of the private attribute types of RADIUS.

show radius vendor-specific

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the configuration of the private attribute types of RADIUS.

Configuration Examples

```
Ruijie# show radius vendor-specific
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 host.
radius-server retransmit	Defines the RADIUS packet retransmission times.

radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the timeout period of RADIUS packet retransmission.

Platform Description N/A

TACACS+ Commands

aaa group server tacacs+

Use this command to configure TACACS+ server groups to group different TACACS+ servers.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Parameter Description

Parameter	Description
group_name	TACACS+ server group name

Defaults

No TACACS+ server group is configured by default.

Command Mode

Global configuration mode

Usage Guide

By dividing TACACS+ servers into several groups, 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 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
server	Configures the server list of a TACACS+ server group.
ip vrf forwarding	Configures the VRF name supported by a TACACS+ server group.

Platform Description

N/A

ip tacacs source-interface

Use this command to configure the source address of a TACACS+ packet.

ip tacacs source-interface *interface*

no ip tacacs source-interface

Parameter

Parameter	Description

Description	*interface*	Source address interface of a TACACS+ packet

Defaults The source address of a TACACS+ packet is set at the network layer by default.

Command Mode Global configuration mode

Usage Guide To decrease the workload of maintaining massive NAS messages on TACACS+ servers, use this command to set the source addresses of TACACS+ packets. This command specifies the first IP address of the specified interface as the source address of a TACACS+ packet and is used on Layer 3 devices.

Configuration Examples The following example configures a TACACS+ packet to obtain an IP address from the interface fastEthernet 0/0 as the source address of the TACACS+ packet.

```
Ruijie(config)# ip tacacs source-interface fastEthernet 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

ip vrf forwarding(TACACS+)

Use this command to configure the VRF name used by a TACACS+ group server (this command is available on the device supporting VRF).

ip vrf forwarding *vrf-name*

no ip vrf forwarding

Parameter Description

Parameter	Description
vrf-name	VRF name

Defaults N/A

Command Mode TACACS+ group server configuration mode

Usage Guide Use this command to configure the VRF name used by a TACACS+ group server.

Configuration The following example specifies the VRF name used by a TACACS+ server group as **vpn1**.

Examples

```
Ruijie(config)# aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
Ruijie(config-gs-tacacs+)# ip vrf forwarding vpn1
```

Related Commands

Command	Description
aaa group server tacacs+	Configures a TACACS+ server group.
server	Configures the server list of a TACACS+ server group.

Platform Description N/A

server(TACACS+)

Use this command to configure the server address in a TACACS+ group server.

server { *ip-address* | *ipv6-address* }

no server { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	server IP address in a TACACS+ group server
ipv6-address	server IPv6 address in a TACACS+ group server

Defaults N/A

Command Mode TACACS+ group server configuration mode

Usage Guide

Before you run this command, run the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

To configure the server address in a TACACS+ group server, you must run the **tacacs-server host** command in global configuration mode.

For the server address in a TACACS+ group server, when a server does not respond, it will send the request to the next server.

Configuration Examples

The following example configures a TACACS+ server group named **tac1** and a TACACS+ server address 1.1.1.1 in this group.

```
Ruijie(config)# aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description
aaa group server tacacs+	Configures a TACACS+ server group.
ip vrf forwarding	Configures the VRF name supported by a TACACS+ server group.

Platform Description N/A

tacacs-server host

Use this command to configure the IP address of a TACACS+ server host.

tacacs-server host {*ip-address* | *ipv6-address*} [**port** *integer*] [**timout** integer] [**key** *string*]

no tacacs-server host {*ip-address* | *ipv6-address*}

Parameter Description

Parameter	Description
Ip-address	IP address of the TACACS+ security server host
ipv6-address	IPv6 address of the TACACS+ security server host
port *integer*	TCP port used in TACACS+ communication
timeout *integer*	Timeout period of the TACACS+ host
key *string*	Shared keyword of the TACACS+ client and server

Defaults No TACACS+ host is specified by default.

Command Mode Global configuration mode

Usage Guide To use TACACS+ to implement the AAA security service, you must define a TACACS+ security server. You can define one or multiple TACACS+ security servers by using the **tacacs-server** command.

Configuration Examples The following example defines a TACACS+ security server host.

```
Ruijie(config)# tacacs-server host 192.168.12.1
Ruijie(config)# tacacs-server host 2001::1
```

Related Commands

Command	Description
aaa authentication	Defines an AAA identity authentication method list.
tacacs-server key	Defines the shared password of TACACS+ security servers globally.
tacacs-server timeout	Defines the timeout timer of reply packets of a TACACS+ server globally.

Platform Description N/A

tacacs-server key

Use this command to configure the global password of TACACS+.

tacacs-server key [*0* | *7*] *string*

no tacacs-server key

Parameter Description

Parameter	Description
string	Text of the shared password
0 | *7*	Password encryption type. 0 indicates no encryption and 7 indicates simple encryption.

Defaults No shared password is specified.

Command Mode Global configuration mode

Usage Guide The device and TACACS+ security server communicates with each other successfully based on the shared password. Therefore, to ensure communication between the device and TACACS+ security server, the same shared password must be defined on both of them. When different passwords must be specified on each server, use the **key** option in the **tacacs-server host** command. You can set a key on each server that does not have **key** option configuration in global configuration mode.

Configuration Examples The following example defines the shared password of a TACACS+ security server as aaa.

```
Ruijie(config)#tacacs-server key aaa
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.
tacacs-server timeout	Defines the timeout timer of TACACS+ packets.

Platform Description N/A

tacacs-server timeout

Use this command to configure the global server timeout period during communicatin with a TACACS+ server.

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter Description

Parameter	Description
seconds	Timeout period (in seconds) in the range from 1 second to 1000 seconds

Defaults The default timeout period is five seconds.

Command Mode Global configuration mode

Usage Guide

Use this command to adjust the timeout period of reply packets. When you need to specify a different timeout period on each server, use the **timeout** option in the **tacacs-server host** command. You can set a timeout period on each server that does not have **timeout** option configuration in global configuration mode.

Configuration Examples

The following example sets the timeout period to 10 seconds.

```
Ruijie(config)# tacacs-server timeout  10
```

Related Commands

Command	Description
tacacs-server host	Defines the TACACS+ security server host.
tacacs-server key	Defines the shared password of TACACS+.

Platform Description

N/A

debug tacacs+

Use this command to turn on the TACACS+ debugging switch.

Use the **no** form of this command to turn off the TACACS+ debugging switch.

debug tacacs+

no debug tacacs+

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

show tacacs

Use this command to query the interoperation with each TACACS+ server.

show tacacs

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A.

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to query the interoperation with each TACACS+ server.

Configuration Examples

```
Ruijie# show tacacs
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Related Commands

Command	Description
tacacs-server host	Defines the TACACS+ security server host.

Platform Description	N/A

SSH Commands

crypto key generate

Use this command to generate a public key on the SSH server in global configuration mode.

crypto key generate {**rsa | dsa**}

Parameter Description

Parameter	Description
rsa	Generates an RSA key.
dsa	Generates a DSA key.

Defaults The SSH server does not generate a public key by default.

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 running the **enable service ssh-server** command at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if an 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

```
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 the DSA and RSA keys and disables the SSH server function.

Platform Description N/A

crypto key zeroize

Use this command to delete the public key on the SSH server in global configuration mode.

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 Use this command to delete the public key on 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

```
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 the DSA and RSA keys.

Platform Description N/A

ip scp server enable

Use this command to enable the SCP server. With the SCP server enabled on a network device, the user can directly download files from the network device and upload local files to the network device. Meanwhile, the user can transfer all interactive data in encrypted text manner, featuring authentication and security.

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 The SCP server is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the SCP server.

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ip ssh authentication-retries

Use this command to set the user 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	User authentication retry times, in the range from 0 to 5

Defaults The default authentication retry times are 3. You can use the **no ip ssh authentication-retries** command to restore the default value.

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 are exceeded. Use the **show ip ssh** command to view the configuration of the SSH server.

Configuration Examples The following example sets the user 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

ip ssh peer

Use this command to associate a public key file with a username. When processing client authentication, the server uses a specified public key file according to the username of the client.

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

ip ssh peer *username* **public-key {rsa | dsa}** *filename*

no ip ssh peer *username* **public-key {rsa | dsa}** *filename*

Parameter Description

Parameter	Description
username	Username
filename	Key file name

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures RSA key file and DSA key file that are associated with username *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
N/A	N/A

Platform Description N/A

ip ssh time-out

Use this command to set the user authentication timeout period on 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	User authentication timeout period

Defaults The default user authentication timeout period is 120 seconds. You can use the **no ip ssh time-out** command to restore the default value.

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 reception of a connection request. Use the **show ip ssh** command to view the configuration of the SSH server.

Configuration Examples The following example sets the timeout period 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

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. When a version is set, only the connection sent by the SSH client of this version is accepted. You can use the **no ip ssh version** command to restore the default setting.

Command Mode Global configuration mode

Usage Guide Use this command to configure the SSH connection protocol version supported by the SSH server. By default, the SSH server supports SSH1 and SSH2, and the clients of these versions can connect to the SSH server. 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 to Version 2.

```
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 N/A

Description

disconnect ssh

Use this command to disconnect the established SSH connection.

disconnect ssh [**vty**] *session-id*

Parameter Description	**Parameter**	**Description**
	session-id	ID of the established SSH connection session

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can disconnect an SSH connection by entering the ID of the SSH connection or the specified VTY connection ID. Only connections of the SSH type can be disconnected.

Configuration Examples

```
Ruijie# disconnect ssh 1  Or
Ruijie# disconnect ssh vty 1
```

Related Commands	**Command**	**Description**
	show ssh	Displays information about the established SSH connection.
	clear line vty *line_number*	Disconnects the current VTY connection.

Platform Description N/A

show crypto key mypubkey

Use this command to query the public key part of the public key on the SSH server.

show crypto key mypubkey {***rsa****dsa*}

Parameter Description	**Parameter**	**Description**
	rsa	Displays the public key part of the RSA key.
	dsa	Displays the public key part of the DSA key.

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the public key part of the generated public key on the SSH server, including the key generation time, key name, and contents of the public key part.

Configuration Examples

```
Ruijie# show crypto key mypubkey rsa
```

Related Commands

Command	Description
crypto key generate {**rsa	dsa**}	Generates the DSA and RSA keys.

Platform Description N/A

show ip ssh

Use this command to query the effective configuration of the SSH server.

show ip ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the effective configuration of the SSH server, including the version, whether the SSH server is enabled, authentication timeout period, 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

```
Ruijie# show ip ssh
```

Related Commands

Command	Description
ip ssh version {**1**	**2**}	Configures the version of the SSH server.
ip ssh time-out time	Sets the user authentication timeout period on the SSH server.
ip ssh authentication-retries	Sets the user authentication retry times on the SSH server.

Platform Description N/A

show ssh

Use this command to query each SSH connection.

show ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query the established SSH connections, including the VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.

Configuration Examples

```
Ruijie# show ssh
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

IP Accounting Commands

clear ip accounting

Use this command to clear IP accounting statistics on the specified interface in privileged EXEC mode.

clear ip accounting interface *interface-type interface-number* { **ingress** | **egress** }

Parameter Description	**Parameter**	**Description**
	interface-type	Type of the specified interface
	interface-number	Number of the specified interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear traffic statistics on the specified interface.

Configuration Examples The following example clears IP accounting statistics on the specified outbound interface.

```
Ruijie# clear ip accounting interface gigabitEthernet 0/1 egress
```

Related Commands	**Command**	**Description**
	show ip accounting interface	Displays IP accounting statistics on the specified interface.

Platform Description N/A

ip accounting

Use this command to enable IP accounting on the specified interface in interface configuration mode. Use the **no** form of this command to disable the function.

ip accounting {**ingress** | **egress**} **list** { *acl_list_number* | *acl_list_name* }

no ip accounting {ingress | egress} [**list** {*acl_list_number* | *acl_list_name*}]

Parameter Description	**Parameter**	**Description**
	acl_ list_ number	ID of the created ACL

Defaults IP accounting is disabled on each interface by default.

Command Mode Interface configuration mode

Usage Guide IP accounting is enabled on the inbound or outbound interface. You need to specify an interface and the direction when enabling IP accounting. In addition, you can configure a traffic classification rule while enabling IP accounting. The system will collect statistics on traffic based on the configured rule.

Configuration Examples The following example enables IP accounting on the outbound interface gi0/1.

```
Ruijie(config)# interface gi0/1
Ruijie(config-if)# ip accounting egress list 10
```

Related Commands

Command	Description
show ip accounting interface	Displays IP accounting configuration on the specified interface.

Platform Description N/A

show ip accounting config

Use this command to query IP accounting configuration on the specified interface in privileged EXEC mode.

show ip accounting config

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query all interfaces on which IP accounting is enabled.

Configuration Examples

```
Ruijie# show ip accounting config
GigabitEthernet 0/1
ip accounting ingress list 20
GigabitEthernet 0/1
ip accounting egress list 10
```

Related Commands

Command	Description
ip accounting { **ingress** | **egress** } **list** { ***acl_list_number*** | ***acl_list_name*** }	Enables IP accounting on the specified interface.

show ip accounting interface

Use this command to query IP accounting statistics on the specified inbound or outbound interface based on a policy.

show ip accounting interface *interface-type interface-number* { **ingress** | **egress** } { **interior** | **exterior** }

Parameter Description

Parameter	Description
interface-type	Type of the specified interface
interface-number	Number of the specified interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to query IP accounting statistics on the specified inbound or outbound interface based on a policy.

Configuration Examples

```
Ruijie# show ip accounting interface gigabitEthernet 0/1 ingress interior
```

Related Commands

Command	Description
clear ip accounting	Clears IP accounting statistics on the specified interface.

Platform Description N/A

Tunnel Interface Commands

keepalive (tunnel interface)

Use this command to enable GRE tunnel keepalive function.

Use the **no** form of this command to disable the function.

keepalive [*seconds* [*retries*]]

no keepalive

Parameter Description

Parameter	Description
seconds	(Optional) Sets the interval (in seconds) of sending keepalive packets. The valid range is from 0 to 32767 and the default value is 10s.
retries	Sets the retry times of sending keepalive packets. The tunnel interface protocol status is DOWN if no reply message is received until the configured retry times are reached. The valid range is from 1 to 255 and the default value is 3.

Defaults

The keepalive function is disabled by default.

If you only input **keepalive** without parameters, the following default values are used:

seconds: 10s

retries: 3

Command Mode

Tunnel interface configuration mode

Usage Guide

Use this command to enable the tunnel keepalive function to detect the reachability of tunnel interfaces. Tunnel packets cannot be sent to the peer end when the physical interface of sending the packets is UP but lines are faulty.

Note

Note that this command is supported in 10.4 (2) and later versions and cannot be used with the **tunnel vrf** and **vrf forward** commands.

Configuration Examples

The following example enables the keepalive function on tunnel interface 1, with the interval and retry times of sending keepalive messages set to 3 seconds and 5 times.

```
Ruijie(config)# interface tunnel 1
Ruijie(config)# keepalive 3 5
```

Related Commands

Command	Description
show interface tunnel	Displays the tunnel interface configuration.

Platform Description N/A

tunnel checksum

Use this command to check data integrity on tunnel interfaces in interface configuration mode.
Use the **no** form of this command to cancel the setting.
tunnel checksum
no tunnel checksum

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is applicable only to Generic Route Encapsulation (GRE) interfaces. Some encapsulated protocols appendix packets with checksum that is automatically added by medium. Checksum verification must be performed on tunnel interfaces. Corrupted packets are discarded directly.

Configuration Examples The following example uses the **checksum** command on tunnel interface 0.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel checksum
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description This command is supported on routers but not switches.

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 remove the configured destination IP address of the tunnel inteface.
tunnel destination *ip-address*
no tunnel destination

Parameter Description

Parameter	Description
ip-address	Sets the IP address of the specified tunnel destination.

Defaults The destination IP address is null 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

tunnel keepalive

Use this command to enable the GRE tunnel keepalive function.

tunnel keepalive *period retries*

no tunnel keepalive

Parameter Description

Parameter	Description
period	Sets the interval (in seconds) of sending keepalive packets. The valid range is from 1 to 65535.
retries	Sets the retry times of sending keepalive packets. The tunnel interface protocol status is DOWN if no reply message is received until the configured retry times are reached. The valid range is from 1 to 1000.

Defaults The keepalive function is disabled by default.

Command Mode Tunnel interface configuration mode

Usage Guide Use this command to enable the tunnel keepalive function to detect the reachability of tunnel interfaces. Tunnel packets cannot be sent to the peer end when the physical interface of sending the

packets is UP but lines are faulty.

Note that this command is supported only in 10.4 (1) and cannot be used with the **tunnel vrf** and **ip vrf forward** commands.

Configuration Examples The following example enables the keepalive function on tunnel interface 1, with the interval and retry times of sending keepalive messages set to 3 seconds and 5 times.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel keepalive 3 5
```

Related Commands

Command	Description
show interface tunnel	Displays the tunnel interface configuration.

Platform Description N/A

tunnel key

Use this command to set the security key on a tunnel interface. The value of the tunnel keyword is an integer.

Use the **no** form of this command to delete the tunnel key.

tunnel key *value*

no tunnel key

Parameter Description

Parameter	Description
value	Tunnel key value, in the range from 0 to 4294967295.

Defaults No key configuration is available by default.

Command Mode Interface configuration mode

Usage Guide Without key protection, illegal intrusion or packet attack may occur during tunnel setup. This command takes effect only when the GRE is encapsulated.

Configuration Examples The following example sets the key of tunnel interface 0 to 1234.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel key 1234
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description This command is supported on routers but not switches.

tunnel mode

Use this command to set the encapsulation mode on a tunnel interface.
Use the **no** form of this command to restore the default value.
tunnel mode { **gre** { **ip** | **ipv6** } | **ipip** | **ipv6ip** }

Parameter Description

Parameter	Description
gre ip	GRE for the route at the IP layer
gre ipv6	GRE for the route at the IPv6 layer
ipip	IP over IP encapsulation mode
ipv6ip	IPv6 over IP encapsulation mode

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

tunnel nested-limit

Use this command to set the maximum number of nested encapsulation layers on a tunnel interface.
tunnel nested-limit *num*
no tunnel nested-limit

Parameter Description

Parameter	Description
num	Maximum number of nested encapsulation layers on a tunnel interface, in the range from 0 to 10

Defaults The maximum number of nested encapsulation layers is four by default.

Command Mode Tunnel interface configuration mode

Usage Guide Tunnel nested encapsulation indicates that packets are sent after multiple-layer tunnel encapsulation on the local device. The route change on the local device may lead to unlimited tunnel nested encapsulation, which causes continuous fragmentation and re-combination on routers and has serious performance impact. RGOS can automatically prevent unlimited nested encapsulation. The maximum number of nested encapsulation layers is four by default. You can use this command to change the default value at the inner layer of a tunnel interface.

Configuration Examples The following example sets the maximum number of GRE nested encapsulation layers on tunnel interface 1 to five.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel nested-limit 5
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description This command is supported on routers.

tunnel path-mtu-discovery

Use this command to activate the tunnel PMTUD function in interface configuration mode.
Use the **no** form of this command to restore the default method.
tunnel path-mtu-discovery [**age-timer** { *aging-mins* | **infinite** } |
min-mtu *mtu-bytes*]
no tunnel path-mtu-discovery [**age-timer | min-mtu**]

Parameter Description

Parameter	Description
aging-mins	(Optional) Sets the MTU aging time on a tunnel interface. After the aging time elapses, a tunnel will send detection packets to detect the path MTU. The valid range is from 10 to 30 (in minutes) and the default value is 10 minutes. When this parameter is set to infinite, the MTU age-timer is disabled.
mtu-bytes	Sets the minimum tunnel interface MTU that can be adjusted by the

	PMTUD function. The valid range is from 92 to 65535 (in bytes) and the default value is 92 bytes.

Defaults The PMTUD function is deactivated on IP tunnel by default.

Command Mode Interface configuration mode

Usage Guide The load protocol packet size may exceed the tunnel interface MTU after encapsulation, leading to packet fragmentation even though the DF bit is set in the header of the load IP packet. Use this command in interface configuration mode to automatically detect the PMTU of the peer tunnel and adjust the MTU size of a tunnel interface, avoiding packet fragmentation.


Note

Note that this command is supported in 10.4 (2) and later versions.
The following states are displayed for PMTUD after the command is executed:
Path MTU Discovery state:init
Path MTU Discovery state:keep
Path MTU Discovery state:learning
They indicate the three state machines in the PMTUD learning process.
The state is init for initial command configuration.
The state changes to learning when detection packets (learning packets) are sent for learning upon timer expiration.
The state changes to keep and keep packets are sent when MTU change is not returned after sending of five consecutive detection packets.

Configuration Examples The following example activates the PMTUD on tunnel interface 0.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

tunnel path-mtu-discovery

Use this command to activate the tunnel PMTUD function in interface configuration mode.
Use the **no** form of this command to disable the function.
tunnel path-mtu-discovery *age-timer min-mtu*
no tunnel path-mtu-discovery

Parameter Description

Parameter	Description
age-timer	Sets the MTU aging time on a tunnel interface. After the aging time elapses, a tunnel will send detection packets to detect the path MTU.
min-mtu	Sets the minimum tunnel interface MTU that can be adjusted by the PMTUD function. The valid range is from 92 to 1500 (in bytes).

Defaults The PMTUD function is deactivated on IP tunnels by default.

Command Mode Interface configuration mode

Usage Guide The load protocol packet size may exceed the tunnel interface MTU after encapsulation, leading to packet fragmentation even though the DF bit is set in the header of the load IP packet. Use this command in interface configuration mode to automatically detect the PMTU of the peer tunnel and adjust the MTU size of the tunnel interface, avoiding packet fragmentation.


Note This command is supported only in10.4 (1).

Configuration Examples The following example activates the PMTUD function on tunnel interface 0.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel path-mtu-discovery 10 100
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

tunnel sequence-datagrams

Use this command to discard packets with sequence errors on a tunnel interface in interface configuration mode.

Use the **no** form of this command to cancel the configuration.

tunnel sequence-datagrams

no tunnel sequence-datagrams

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is valid only for GRE. The RGOS allows configuration of receiving rules for tunnels to directly discard packets with sequence errors. Use this command to implement sequential packet transmission for some load protocols lacking in packet sequence maintenance.

Configuration Examples The following example uses the **tunnel sequence-datagrams** command on tunnel interface 0.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel sequence-datagrams
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description This command is supported on routers but not on switches.

tunnel source

Use this command to set the source address of a tunnel interface in interface configuration mode.
Use the **no** form of this command to remove the source address of the tunnel interface.
tunnel source { *ip-address* | *interface-type interface-number* }
no tunnel source

Parameter Description

Parameter	Description
ip-address	Source IP address of a tunnel interface, which is the IP address of other interface configured on a router
interface-type	Interface type, such as Async, Dialer, Ethernet, FastEthernet, Loopback, Null, and other tunnel interface types
interface-number	Interface number.

Defaults No source address is specified by defaults.

Command Mode Interface configuration mode

Usage Guide The source address of a tunnel interface in use must be specified.

Configuration Examples The following example specifies the serial port 1/0 as the source address of tunnel interface 0.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel source serial 1/0
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description	N/A

tunnel tos

Use this command to set the IPv4 ToS byte or IPv6 traffic class 8 bits fin tunnel inteffface configruation mode.

tunnel tos [*num*]

no tunnel tos

Parameter Description	**Parameter**	**Description**
	num	IPv4 ToS byte or IPv6 traffic class 8 bits. The valid range is from 0 to 255.

Defaults By default, the inner-layer IPv4 ToS byte is copied to the outer-layer IPv4 header, if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the IPv4 protocol. By default, the inner-layer IPv6 traffic class 8 bits are copied to the outer-layer IPv6 header if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the Ipv6 protocol.
In other circumstances, the outer-layer IPv4 ToS and IPv6 traffic class are 0.

Command Mode Interface configuration mode

Usage Guide The administrator can use this command to set GRE tunnel packets to a higher priority.


Note This command is supported in 10.4 (2) and later versions.

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

tunnel ttl

Use this command to set the TTL value on a tunnel interface in interface configuration mode.

Use the **no** form of this command to restore the default value.

tunnel ttl *hop-count*

no tunnel ttl

Parameter Description	Parameter	Description
	hop-count	Specifies the TTL value of a tunnel interface.

Defaults The default TTL values of tunnel interfaces are 255.

Command Mode Interface configuration mode

Usage Guide The point-to-point link tunnel interface using a load protocol costs more than one route hop for actual transmission. The RGOS allows configuration of the tunnel TTL value, that is, the TTL value in the header of a TCP packet encapsulated on the tunnel. The TTL value in the header of a TCP packet is reduced by a router in the intermediate node of the tunnel, and the packets whose TTL values are 0 are discarded.

Configuration Examples The following example sets the TTL value on tunnel interface 0 to 16.

```
Ruijie(config)# interface tunnel 0
Ruijie(config-if)# tunnel ttl 16
```

Related Commands	Command	Description
	show interfaces tunnel	Displays tunnel interface information.

Platform Description N/A

tunnel vrf

Use this command to set the IPv4 VRF for routing and forwarding.

tunnel vrf [*vrf-name*]

no tunnel vrf

Parameter Description	Parameter	Description
	vrf-name	IPv4 VRF name

Defaults IPv4 uses the global VRF table for routing and forwarding by default.

Command Mode Interface configuration mode

Usage Guide The source and destination IP addresses for outer-layer tunnel encapsulation must be in the same VRF. If there is no reachable route for the destination IP address in the specified VRF, the tunnel

interface is down.

Note This command is supported in 10.4 (2) and later versions.

Configuration Examples The following example sets IPv4 VRF blue for routing on tunnel interface 1.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel vrf blue
```

Related Commands

Command	Description
show interfaces tunnel	Displays tunnel interface information.

Platform Description N/A

show tunnel gre

Use this command to query GRE tunnel configuration in the summary view.

show tunnel gre

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command when you need to query the number of GRE tunnels configured on the local device in the case of massive operation configurations. This spares the need of analyzing massive show running information.

Configuration Examples The following example displays the number of GRE tunnels configured on the local device and information about each tunnel in the summary view.

```
Ruijie# show tunnel gre
Tunnel1:
Mode:GRE/IP, Destination 192.168.2.2, Source vlan 100
```

Related Commands

Command	Description
show interfaces tunnel	Displays tunnel interface information.

Platform Description N/A

SDG Commands

clear user-group

Use this command to clear users in a user group in privileged EXEC mode.

clear user-group *group-name*

Parameter Description

Parameter	Description
group-name	Name of a user group

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to remove users of default configuration or the users added during SDG initiative/passive access in local mode.
Use this command to remove all users in a user group in link mode.

Configuration Examples

```
Ruijie#clear user-group intranet_user
Ruijie#clear user-group internet_user
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on RSR series router products.

ip sdg classifier

Use this command to define an SDG classifier in global configuration mode and enter SDG classifier configuration mode.
Use **no** form of this command to remove an SDG classifier.
ip sdg classifier *classifier-id*
no ip sdg classifier *classifier-id*

Parameter Description

Parameter	Description
classifier-id	Classifier ID

Defaults N/A

Command Mode Global configuration mode

Usage Guide To control the SDG, you must first define SDG classifiers. Each SDG classifier defines a series of user groups (user roles). A user can only belong to one user group at a time.
The created SDG classifier is applied to the SDG policy. When user access violates the SDG policy, the user selection page will be triggered to prompt the user to select a user group.
The user can also access the user selection page to select a user group. The URL of the user selection page is:
"http://" + device interface address + "/sdg" + classifier ID + ".htm". For example, if the interface address is 192.168.52.52 and the classifier ID is 1, then the corresponding URL is:
http://192.168.52.52/sdg001.htm?ruijie_query_id=sdg


Caution

The Web server functiojn must be enabled in order to generate the user role selection page.

```
Ruijie(config)# enable service web-server
```

Configuration Examples The following example creates an SDG classifier with the ID 1.

```
Ruijie(config)# ip sdg classifier 1
Ruijie(config-sdg-classifier)# exit
```

Related Commands

Command	Description
ip sdg in|out access-group *acl-no* trigger *classifier-id*	Applies a classifier to the SDG policy.

Platform Description This command is supported only on RSR series router products.

ip sdg dns-hijack

Use this command to enable DNS hijacking. Use the **no** form of this command to restore the default setting.

ip sdg dns-hijack interface loopback *num* **action { drop | permit }**

no ip sdg dns-hijack

Parameter Description

Parameter	Description
num	Loopback interface ID
drop	All DNS query packets except Class A DNS query packets are discarded.
permit	All DNS query except class A query packets are forwarded.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Configure DNS hihacking in correlation mode.
Ensure that the loopback interface is up.

Configuration Examples The following example enables DNS hijacking.

```
Ruijie(config)# ip sdg dns-hijack interface loopback 0 action drop
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip sdg in|out

Use this command to define an SDG policy on the specified interface in interface configuration mode.

ip sdg in|out access-group *acl-no* **trigger** *classifier-id*

Parameter Description

Parameter	Description
acl-no	ACL number
classifier-id	SDG classifier ID

Defaults N/A

Command Mode Interface configuration mode

Usage Guide Before defining an SDG policy, use the ACL to define an isolation policy, which must be based on user groups included in the SDG classifier.
When user access violates the isolation policy, the user selection page defined in the SDG policy will be triggered to prompt the user to select a proper user group.

Configuration Examples

```
Ruijie(config)#interface gigabitEthernet 0/0
Ruijie(config-if-gigabitEthernet 0/0)#ip sdg in access-group 100 trigger 1
```

Related Commands

Command	Description
ip access-list	Defines the ACL reflecting the isolation policy.
ip sdg classifier	Defines the SDG classifier.

Platform Description This command is supported only on RSR series router products.

ip sdg mode

Use this command to select an SDG operating mode, including the local mode and link mode, in global configuration mode.
ip sdg mode { **local** | **link** }
no ip sdg mode { **local** | **link** }

Parameter Description

Parameter	Description
local	Local mode
link	Link mode

Defaults The default SDG operating mode is the local mode.

Command Mode Global configuration mode

Usage Guide

During switching of the SDG operating mode, the user information in original mode will be cleared.

Configuration Examples The following example enables the SDG link mode.

```
Ruijie(config)# ip sdg mode link
```

Related

Command	Description

Commands	N/A	N/A

Platform Description This command is supported only on RSR series router products.

ip sdg offline-detect

Use this command to configure the keepalive duration and threshold of user traffic. Use the **no** form of this command to restore the default setting.

ip sdg offline-detect idle-timeout *time-out* **threshold** *flow-num*

no ip sdg offline-detect

Parameter Description

Parameter	Description
time-out	Range: 1-65535 Min. Default: 15 Min
flow-num	Range: 1-4294967294B. Default: 1024B

Defaults N/A

Command Mode Global configuration mode

Usage Guide Configure the keepalive duration and threshold of user traffic in correlation mode.

Configuration Examples The following example configures the keepalive duration and threshold of user traffic.

```
Ruijie(config)# ip sdg offline-detect idle-timeout 2 threshold 2048
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip sdg portal

Use this command to configure the authentication address of the eportal server and the port address of the router that communicates with the eportal server.

ip sdg portal *ip* [*url*]

no ip sdg portal

Parameter Description

Parameter	Description
ip	IP address of the router's port that communicates with the eportal server
url	URL of the authentication page of the eportal server

Defaults NA

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the SMP address.

```
Ruijie(config)# ip sdg portal 10.1.1.2 http://www.xxx.gov/eportal
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on RSR series router products.

ip sdg permit-user

Use this command to configure the IP address of the default user group in the SDG classifier in SDG classifier configuration mode.

ip sdg permit-user *ip mask* user-group *group_name*

no ip sdg permit-user *ip mask* user-group *group_name*

Parameter Description

Parameter	Description
group-name	Name of the default user group
ip	IP network segment of users
mask	IP mask of users (the minimum mask that can be used is 21 bits)

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

The following example adds a member to the default user group intranet_user in the SDG classifier with the ID 1.

```
Ruijie(config)#ip sdg permit-user 192.168.52.0 255.255.255.0 user-group intranet_user
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on RSR series router products.

ip sdg user-timeout

Use this command in global configuration mode to configure the time after which the SDG link user is considered down if no connection is detected after all connections of this user have been terminated.

ip sdg user-timeout *time*

no ip sdg user-timeout

Parameter Description

Parameter	Description
time	In the range from 1 minute to 30 minutes

Defaults

10 minutes

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the user-timeout period to 5 minutes.

```
Ruijie(config)# ip sdg user-timeout 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on RSR series router products.

user-group

Use this command to configure the user groups included in the SDG classifier in SDG classifier

configuration mode.

Use **no** form of this command to remove the specified user group.

user-group *group-name*

no user-group *group-name*

Parameter Description

Parameter	Description
group-name	Name of a user group

Defaults

N/A

Command Mode

SDG classifier configuration mode

Usage Guide

After creating the SDG classifier, use this command to configure the user groups included in the SDG classifier.

Caution The user groups defined in the SDG classifier must have been created already.

Configuration Examples

The following example adds two user groups (internet_user and intranet_user) to the SDG classifier with the ID 1.

```
Ruijie(config)# ip sdg classifier 1
Ruijie(config-sdg-classifier)# user-group internet_user
Ruijie(config-sdg-classifier)# user-group intranet_user
Ruijie(config-sdg-classifier)# exit
```

Related Commands

Command	Description
ip sdg classifier *classifier-id*	Defines the SDG classifier.

Platform Description

This command is supported only on RSR series router products.

Anti-attack Commands

acpp

Use this command to configrue aggregate control plane protection (ACPP) in control-plane configuration mode.
Use the **no** form of this command to cancel the ACPP rule.
acpp bw-rate *rate* **bw-burst-rate** *burst-rate*
no acpp

Parameter Description

Parameter	Description
rate	Rate limit, in pps
burst-rate	Burst rate limit, in pps

Defaults ACPP is disabled by default.

Command Mode Control-plane configuration mode. You can configure it on three sub-interfaces.

Usage Guide N/A

Configuration Examples The following example sets the traffic rate to 200 pps and the burst rate to 300 pps for configuration services.

```
Ruijie(config)# control-plane data
Ruijie(config-cp)# acpp bw-rate 200 bw-burst-rate 300
```

Related Commands

Command	Description
Ruijie(config)# **control-plane** [**protocol** | **manage** | **data**]	Enters control-plane configuration mode and the corresponding sub-interface.

Platform Description N/A

arp-car

Use this command to configure ARP-CAR rate limit for received ARP packets in control-plane configuration mode.
Use the **no** form of this command to remove ARP-CAR rules.
arp-car *packet_rate_per_group*
no arp-car

Parameter Description	Parameter	Description
	packet_rate_per_group	Rate limit, in pps

Defaults ARP-CAR is disabled by default.

Command Mode Control-plane configuration mode. You can configure it only on the management sub-interfaces.

Usage Guide N/A

Configuration Examples The following example limits the rate to 5 pps for ARP traffic originated by users (source) in the same group through the HASH algorithm.

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# arp-car 10
```

Related Commands	Command	Description
	Ruijie(config)# **control-plane** [**protocol** | **manage** | **data**]	Enters control-plane configuration mode and the corresponding sub-interface.

Platform Description N/A

control-plane

Use this command to enter control-plane configuration mode.
Use the **exit** command to quit control-plane configuration mode.
control-plane { **protocol** | **manage** | **data** }

Parameter Description	Parameter	Description
	protocol	Enters protocol control sub-interfaces.
	manage	Enters management sub-interfaces.
	data	Enters service sub-interfaces.

Defaults N/A

Command Mode Global configuration mode

Usage Guide When you enter control-plane configuration mode without any parameters configured, you can enable the default rule switch for anti-attack on equipment.

Configuration Examples The following example enters control-plane configuration mode and the protocol control sub-interfaces.

```
Ruijie(config)# control-plane protocol
```

```
Ruijie(config-cp)#
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ef-rnfp

Use this command to enable anti-attack with default rules and policies.
Use the **ef-rnfp disable** command to disable anti-attack and clear related rules.
ef-rnfp enable
ef-rnfp disable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults Anti-attack is disabled by default.

Command Mode Control-plane configuration mode

Usage Guide N/A

Configuration Examples The following example disables anti-attack and clears related rules.

```
Ruijie(config)# control-plane
Ruijie(config-cp)# ef-rnfp disable
```

Related Commands	Command	Description
	Ruijie(config)# **control-plane** [**protocol** | **manage** | **data**]	Enters control-plane configruation mode and the corresponding sub-interface.

Plarform Description N/A

glean-car

Use this command in control-plane configuration mode to configure Glean-CAR rate limit for traffic that is distributed to direct routes after routing but whose IP addresses have not be resolved.
Use the **no** form of this command to remove Glean-CAR rules.
glean-car *packet_rate_per_group*
no glean-car

Parameter Description	Parameter	Description
	packet_rate_per_group	Rate limit, in pps

Defaults Glean-CAR is disabled by default.

Command Mode Control-plane configuration mode. You can configure it only on the service sub-interfaces.

Usage Guide N/A

Configuration Examples The following example sets the rate limit to 10 pps for Glean-adjacent traffic originated by users (source) in the same group through the HASH algorithm.

```
Ruijie(config)# control-plane data
Ruijie(config-cp)# glean-car 10
```

Related Commands	Command	Description
	Ruijie(config)# **control-plane** [**protocol** | **manage** | **data**]	Enters control-plane configuration mode and the corresponding sub-interface.

Platform Description N/A

management-interface

Use this command to configure management plane protection (MPP) in control-plane configuration mode. MPP allows administrators to specify one or more interfaces as inband management interfaces (that can receive management packets and forward normal services). After MPP is enabled, only specified inband management interfaces can receive management packets of specified protocols.

Use the **no** form of this command to remove inband management interfaces.

management-interface *interface* **allow** { **ftp** | **http** | **https** | **ssh** | **snmp** | **telnet** | **tftp** }

no management-interface *interface*

Parameter Description	Parameter	Description
	Interface	Specified management interface

Defaults MPP is disabled by default.

Command Mode Control-plane configuration mode. You can configure it only on the management sub-interfaces.

Usage Guide N/A

Configuration The following example specifies gi0/0 as the inband management interface. Only this interface can

Examples receive Telnet and SNMP packets.

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# management-interface gi 0/0 allow snmp telnet
```

Related Commands

Command	Description
Ruijie(config)# **control-plane** [**protocol** | **manage** | **data**]	Enters control-plane configuration mode and the corresponding sub-interface.

Platform Description N/A

port-filter

Use this coomand to confugrue the port filter function in control-plane configuration mode. The port filter function can filter out the arriving illegal transfer-layer packets, whose destination ports are not opened after arrival.

Use the **no** form of this command to disable the function.

port-filter

no port-filter

Parameter Description

Parameter	Description
N/A	N/A

Defaults The port filter function is disabled by default.

Command Mode Control-plane configuration mode. You can configure it only on the management sub-interfaces.

Usage Guide N/A

Configuration Examples The following example enables the port filter function on a management sub-interface.

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# port-filter
```

Related commands

Command	Description
Ruijie(config)# **control-plane** { **protocol** | **manage** | **data** }	To enter control plane mode and the relevant sub-interface.

Platform Description N/A

scpp

Use this command to configure sorted control plane protection (SCPP) in control-plane configuration

mode. SCCP is used for further traffic classification and rate limit in different types of traffic based on policies, for example, connection limit, semi-connection limit, and traffic bandwidth limit.

Use the **no** form of this command to remove SCCP rules.

scpp list *acl_no* { **bw-rate** *bw-rate* **bw-burst-rate** *bw-burst-rate* | **conn-total** *conn-num* | **conn-create-rate** *conn-create-rate* **conn-create-burst-rate** *conn-create-burst-rate* }

no scpp list *acl_no*

Parameter Description

Parameter	Description
acl_no	Match policy that differentiates and limits traffic
bw-rate	Rate limit, in pps
bw-burst-rate	Burst rate limit, in pps
conn-num	Connections limit, in pieces
conn-create-rate	Connection creation limit, in piece/s
conn-create-burst-rate	Connection creation burst rate limit, in piece/s

Defaults SCPP is disabled by default.

Command mode Control-plane configuration mode. You can configure it on three sub-interfaces.

Usage Guide N/A

Configuration Examples The following example sets the rate limit to 100 pps and the burst value to 150 pps on management sub-interfaces for TCP traffic originating from the network segment 192.168.52.0 to the local management sub-interface. The example also sets the connections limit to 30, connection creation rate to 5 piece/s, and connection creation burst rate limit to 7 piece/s.

```
Ruijie(config)# access-list 100 permit tcp 192.168.52.0 0.0.0.255 any
Ruijie(config)# control-plane manage
Ruijie(config-cp)# scpp list 100 bw-rate 100 bw-burst-rate 150 conn-total 30
conn-create-rate 5 conn-create-burst-rate 7
```

Related Commands

Command	Description
Ruijie(config)# **control-plane** [**protocol** | **manage** | **data**]	Enters control-plane configuration mode and the corresponding sub-interface.

Platform Description N/A

show ef-rnfp

Use this command to view the rule configuration and statistics of the anti-attack function.

show ef-rnfp { **acpp** | **scpp** | **glean-car** | **arp-car** | **port-filter** | **mpp** | **all** }

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 configuration and statistics of the anti-attack function.

```
Ruijie# show ef-rnfp all
Aggregate control plane protection information:    //ACPP configuration and
statistics
  Data subinterface: enable
    RULE:
      bandwidth rate limit: 20(pps), burst: 30(pps)
          STATISTIC:
      dropped 0 packets
  Manage subinterface: enable
    RULE:
      bandwidth rate limit: 1000(pps), burst: 2000(pps)
    STATISTIC:
      dropped 0 packets
  Protocol subinterface: disable
Segregate control plane protection information:    //SCPP configuration and
statistics
  Data subinterface: disable
  Manage subinterface: enable
    RULE: acl: 1, id: 1011a4f
      bandwidth rate limit: 20(pps), burst: 300(pps)
     STATISTIC:
      bandwidth rate limit dropped 0 packets
    TOTALLY dropped 0 packets
  Protocol subinterface: disable
ARP CAR information:    //ARP-CAR configuration and statistics
  Manage subinterface: enable
    RULE:
      allow packet rate per source: 30(pps)
        STATISTIC:
      dropped 181 packets
Glean CAR information: //Glean-CAR configuration and statistics
  Data subinterface: disable
Port Filter information:
  Manage subinterface: disable
Management plane protection information:   //MPP     configuration     and
```

```
statistics
  Manage subinterface: disable


-----------------------------------------------------
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

RPL Commands

ip reverse-path

Use this command to enable reverse path limited (RPL) on an interface.

ip reverse-path [**access-list**] [*acl_id*]

Parameter Description

Parameter	Description
acl_id	(Optional) ID of the access control list (ACL): 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)

Defaults RPL is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command applies to layer-3 interfaces and new paths.

Configuration Examples The following example configures the RPL command on an interface.

```
Ruijie(config)# interface gigabitEthernet 0/0
Ruijie(config-GigabitEthernet 0/0)#ip reverse-path
```

Caution Before enabling this command on a subinterface, ensure that the MAC address of the peer subinterface is learnt by this subinterface. If not, the one-way audio failure will occur. You can ping the IP address of the peer subinterface, or use the **shutdown** command to disable the primary interface of the subinterface and then use the **no shutdown** command to enable the primary interface. The preceding restriction does not apply when this command is configured on other interfaces.

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on routers.

QoS Configuration Commands

QoS Commands

bandwidth (policy-map class)

Use this command to allocate bandwidth to the class map referenced in the policy map. Use the **no** form of this command to remove the settings.

bandwidth { *bandwidth-kbps* | **percent** *percent* }

no bandwidth

Parameter Description

Parameter	Description
bandwidth-kbps	Bandwidth allocated to the class map referenced (in Kbps).
percent	Bandwidth percentage allocated to the class map referenced.

Defaults By default, the system allocates no bandwidth to the referenced class map.

Command Mode Policy-map class interface configuration mode.

Usage Guide

This command is used to allocate bandwidth to the referenced class map in the policy map. The bandwidth will be used to identify the weight (priority) of this type of network traffic.
The system has not allocated default bandwidth to the class map referenced in the policy map. If you have not allocated bandwidth to the referenced class map, the system will always allocate 1% of the total available bnadwidth on the network interface when it identifies this type of network traffic.
The total bandwidth occupied by all class maps referenced in the policy map should not exceed the bandwidth allocated to the CBWFQ of the network interface to which the policy map is applied. Otherwise, the network interface will automatically no longer use the policy map. Similarly, the dynamic change of the bandwidth occupied by the class map referenced in the policy map will also cause such impact.

Configuration Examples The following example references the class map acl22 in the policy map polmap6 and allocates 2000 kbps to it.

```
policy-map polmap6
class acl22
bandwidth 2000
queue-limit 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

bandwidth-mode

Use this command to set Car token bucket algorithm mode.

bandwidth-mode car { **link-header** | **frame-gap** }

Parameter Description

Parameter	Description
link-header	Frame gap is excluded in Car token bucket algorithm.
frame-gap	Frame gap is included in Car token bucket algorithm.

Defaults By default, Car token bucket algorithm mode is link-header.

Command Mode Global mode

Usage Guide N/A

Configuration Examples In the following examples, Frame gap is included in Car token bucket algorithm.

```
Ruijie(config)#bandwidth-mode car frame-gap
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

class-map

Use this command to enter the specific class map configuration mode. If the specific class map is not available, the system will create it The **no** form of this command deletes the specific class map.

class-map *class-map-name* [**match-all | match-any**]

no class-map *class-map-name* [**match-all | match-any**]

Parameter Description

Parameter	Description
class-map-name	Name or ID of the class map
**match-all	match-any**	Match all or any rules of the class map.

Defaults By default, no class map is set.

Command Mode Global configuration mode

Usage Guide The **class-map** command allows you to create a specific class map and enter the class-map interface configuration mode, where you can configure match rules to classify data flows. After data flows arrive the specified CBWFQ-enabled interface, they are classified by the rules of the class map. You can classify data flows in the following six ways:

1. match access-group
2. match input-interface
3. match protocol
4. match ip dscp
5. match ip precedence
6. match not match-type value
You can set match rules of a class map for many times. and the rule takes effect according to type of the class map.

Configuration Examples

In the following example, any packets matching ACL 101 are considered as meeting the classification rule of class-map class 1 and be put into the corresponding CBWFQ queue.

```
class-map match-all class1
match access-group 101
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

class (policy-map)

Use this command to enter the referenced specific class map configuration mode. If it is not available, the system will display an error message. If the specific class map is not referenced, the system will add it to the reference list of the corresponding policy map. The **no** form of this command cancels the application of the specific class map from the corresponding policy map.

class class-name

no class class-name

Parameter Description

Parameter	Description
class-name	Name of the referenced class map

Defaults N/A

Command Mode Policy-map interface configuration mode

Usage Guide

The class map referenced in the policy map must be available. Otherwise, you cannot successfully reference it in the policy map. Similarly, if the class map is cleared from the device, all references of this class map will fail, and thus affecting the CBWFQ.
In a policy map table, up to 64 different class maps can be referenced at the same time. After you enter the referenced class map configuration layer of the specified name, you can define the bandwidth allocated to this type of network traffic in the current policy map and the length of the corresponding CBWFQ queue.

Configuration Examples

In the following example, the policy map "policy1" references the class map "acl120" and "acl121". For "acl120", the bandwidth of 600kbps is allocated, and the corresponding CBWFQ queue depth is 64 (system default). For "acl121", the 30% of the interface available bandwidth is allocated, and the corresponding CBWFQ queue depth is 40.

```
policy-map policy1
class acl120
bandwidth 600
class acl121
bandwidth percent 30
queue-limit 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

custom-queue-list

In the interface configuration mode, use this command to apply the custom queue list to the interface. The **no** form of this command is used to restore it to the default settings.

custom-queue-list *list-number*

no custom-queue-list

Parameter Description

Parameter	Description
list-number	Queue list number, an integer in the range of 1 to 16

Defaults

N/A.

Command Mode

Interface configuration mode.

Usage Guide

An interface can have only one queue list.

Configuration Examples

The following example shows how to apply the custom queue list 6 to the synchronous interface 1:

```
Ruijie(config)#interface serial 1
Ruijie(config-if)#custom-queue-list 6
```

Related Commands

Command	Description
priority-list interface	Allocate packets to the specified priority list according to interface type.
queue-list default	Allocate the packets not matching any rules in the custom queue list to a custom queue.

queue-list interface	Allocate packets to the specified custom queue according to the type of the interface where the packets arrive.
queue-list queue byte-count	Specify the number of packet bytes that can be sent continuously while polling the queue
queue-list queue limit	Specify the maximum number of packets that a custom queue can accommodate.
show interfaces	Show the statistics of all the interfaces of the device.
show queue	Show the queue status on the specified interface.

Platform Description N/A

debug ip rtp

Use this command to turn the RTP message compression debugging switch. The **no** form of this command turns off the debugging switch.

debug ip rtp {**header-compression** | **errors**}

no debug ip rtp { **header-compression** | **errors** }

Parameter Description

Parameter	Description
header-compression	Turn on the RTP message compression debugging switch.
errors	Turn on the RTP error message compression debugging switch.

Defaults Disabled

Command Mode Privileged EXEC mode

Usage Guide N/A.

Configuration Examples The following example shows how to turn on the RTP packet compression debugging switch:

```
Ruijie# debug ip rtp header-compression
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug ip tcp

Use this command to turn on the TCP message compression debugging switch. The **no** form of this command turns off the debugging switch.

debug ip tcp {header-compression }

no debug ip tcp { header-compression }

Parameter Description

Parameter	Description
header-compression	Turn on the TCP packet compression debugging switch.

Defaults Disabled.

Command Mode Privileged EXEC mode

Usage Guide N/A.

Configuration Examples The following example shows how to turn the TCP packet compression debugging switch:

```
Ruijie# debug ip tcp header-compression
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A.

debug qos

Use this command to turn on the QoS debugging switch. The **no** form of this command turns off the debugging switch.

debug qos {cq | wfq |cbwfq}

no debug qos {cq | wfq | cbwfq}

Parameter Description

Parameter	Description
cq	Debug CQ or PQ packets.
wfq	Debug WFQ packets.
cbwfq	Debug CBWFQ packets.

Defaults Disabled.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows how to turn on the QoS debugging switch.

```
Ruijie# debug qos cq
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

drop

Use this command to configure the drop rule in the class map configuration mode. The **no** form of this command removes the settings.

drop

no drop

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Policy-map interface configuration mode

Usage Guide Once the traffic is dropped according to a rule of the policy map, you cannot specify any other operation for them.

Configuration Examples The following example drops the traffic matching class c1 on the synchronous interface.

```
Ruijie(config)# class-map class1
Ruijie(config-cmap)# match access-group 101
Ruijie(config-cmap)# policy-map policy1
Ruijie(config-pmap)# class c1
Ruijie(config-pmap-c)# drop
Ruijie(config-pmap-c)# interface s2/0
Ruijie(config-if)# service-policy output policy1
Ruijie(config-if)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

fair-queue

In the interface configuration mode, use the **fair-queue** command to configure the weighted fair queue. The no form of this command removes the setting.

fair-queue [congestive-discard-threshold [dynamic-queues]]

no fair-queue

Parameter Description

Parameter	Description
congestive-discard-threshold	(Optional) Maximum number (threshold) of packets that each queue can accommodate. Its default value is 64. A new threshold must be the power of 1 to 4096. When the number of packets reaches the threshold, the new packets arriving will be discarded.
dynamic-queues	(Optional) Number of the dynamic queues, an integer within 1 to 4096, 256 by default.

Defaults

WFQ is used for a serial interface whose bandwidth is 2.048Mbps or lower by default. However, it does not apply to the following types of interfaces:

1. X.25 encapsulation
2. LAPB
3. Tunnel
4. Lookback
5. Dialer
6. Bridge
7. Virtual interface

The fair queue is not available for the above mentioned protocols.

Command Mode

Interface configuration mode

Usage Guide

In the interface configuration mode, use the command **fair-queue** to configure WFQ for a specific interface.

To configure WFQ congestion management policy on the interface, all interfaces of the system must have the same express forwarding configuration (all enabling or disabling express forwarding), or else the congestion management policy may fail.

The number of dynamic queues must be adjusted according to the current traffic conditions, and the number of dynamic queues must be greater than the service traffic, or else the excess traffic will flow into the same dynamic queue. It is suggested that the number configured to be greater than the number of existing services, and the total number must be no less than 64.

Configuration Examples

The following example shows how to configure the fair queue on the sync interface 0. The congestion discard threshold is 128 messages and 512 dynamic queues:

```
Ruijie(config)#interface Serial 0
Ruijie(config-if)#fair-queue 128 512
```

Related Commands

Command	Description
custom-queue-list	Apply the custom queue list to the interface.
priority-group	Apply the priority list to the interface.
priority-list default	Allocate the packets not matching any rules in the custom queue list to a custom queue.
show interfaces	Show the statistics of all the interfaces of the device.
show queue	Show the queue status of the specified interface..

Platform Description

N/A

flow-label (config-crypto-map)

Use the **fair-queue** command to specify flow numbers for services in the IPSec encyption mapping table. The **no** form of this command removes the setting.

flow-label *label-num*

no flow-label

Parameter Description

Parameter	Description
label-num	Label number of IPSec flow

Defaults

By default, no flow number is specified.

Command Mode

config-crypto-map configuration mode

Usage Guide

This function can specify numbers for services in the IPSec encyption mapping table and implement QoS processing based on IPSec services. Combined with the rate limiting template, this function can implement rate limiting for service flows based on the IPSec tunnel.

Configuration Examples

The following example shows how to set the flow number to 3:

```
crypto map mymap 1 ipsec-isakmp
flow-label 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

flow-limit

Use the **flow-limit** command to configure the global rate limiting template. The **no** form of this command deletes the setting.

flow-limit {**input** | **output**} **label** *label-value bps burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

no flow-limit {**input** | **output**} **qos-group** *group-value bps burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

Parameter Description

Parameter	Description
input|output	Input or output traffic that a user hopes to limit
bps	Rate upper limit that a user hopes, in the unit of bps
burst-normal burst-max	Size of a token bucket, in the unit of byte
conform-action	Processing policy for the traffic below the rate limit
exceed-action	Processing policy for the traffic beyond the rate limit
action	Processing policy, which includes the following:
drop	Discard a packet
transmit	Send a packet.

Defaults By default, no rate limiting template is specified.

Command Mode Global configuration mode

Usage Guide The rate limiting template is provided by QoS to the IP application module to support rate limiting by the IP application. The application module needs to support this function to make the rate limiting rule take effect. At present, the application supporting the rate limiting rule is the IPSec service. The rate limiting template itself has no rate limiting effect, and the application module is required to support the rate limiting function. During configuration, the application module specifies the flow number within its policy and then limits the rate of service flows by using the rate limiting template.

Configuration Examples The following example configures the rate limiting template:

```
flow-limit output label 3 300000 3000 3000 conform-action  transmit
exceed-action  drop
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

hold-queue

In interface configuration mode, use the **hold-queue** command to set the length of the FIFO queue.

hold-queue *queue length* { **in | out** }

no hold-queue [*queue length*] { **in | out** }

Parameter Description

Parameter	Description
queue length	The maximum number (threshold) of data packets that can be contained in a queue. The defualt value is 75 for an incoming queue and 40 for an outgoing queue. After the number of data packets reaches the threshold, new data packets will be discarded.

Defaults The default value is 75 for an incoming queue and 40 for an outgoing queue.

Command Mode Interface configuration mode

Usage Guide In interface configuration mode, use the hold-queue command to set the length of the FIFO queue for a given interface.

Caution This command is used to modify three color-based thresholds of a queue for interface congestion and prevent green packets drop preferentially. In general, you can apply the default settings. Make sure that the number of cached packets is below the red threshold.

Configuration Examples The following example shows how to configure the FIFO queue on the sync interface 0. The congestion discard threshold is 128 messages and 512 dynamic queues:

```
Ruijie(config)# interface Serial 0
Ruijie(config-if)# hold-queue 128 in
```

Related Commands

Command	Description
show interfaces	Display statistics data of all interfaces of a device.

Platform Description N/A

ip rtp compression-connections

In interface configuration mode, use the **ip rtp compression-connections** command to set the number of connections between the compression and decompression of RTP packets. Use the **no** form of this command to restore the default value.

ip rtp compression-connections { *number* }

no ip rtp compression-connections

Parameter Description

Parameter	Description
number	Number of connections between compression and decompression of RTP packets.

Defaults The default number of connections is used.

Command Mode Interface configuration mode.

Usage Guide The default number of connections is used if the command **ip rtp compression-connections** is not configured. By default, the number for PPP and HDLC is 16 and the number for Frame-relay is 256.

Configuration Examples The following example shows how to configure the connections for RTP packets on the sync interface:

```
Ruijie (config)# interface serial 1/0
Ruijie (config-if)# ip rtp compression-connections 25
```

Related Commands

Command	Description
ip rtp header-compression	Configure RTP packet compressions on the interface.
ip tcp compression-connections	Configure the number of TCP comprssion connections.
show ip rtp header-compression	Show the statistics of IP RTP packet compressions on the interface.

Platform Description N/A

ip rtp header-compression

In interface configuration mode, use the **ip rtp header-compression** command to apply RTP packet compression on the interface. Use the **no** form of this command to cancel the configuration.

ip rtp header-compression [**iphc-format** | **passive**]

no ip rtp header-compression

Parameter Description

Parameter	Description
iphc-format	Packet in IPHC format to be compressed.
passive	Passive mode for packet compression.

Defaults No RTP packets are compressed.

Command Mode Interface configuration mode.

Usage Guide After **ip rtp header-compression** is configured, the **iphc-format** option and the **ip tcp header-comopression iphc-format** command are automatically added.

Configuration Examples

The following example shows how to configure RTP packet compression on the sync interface:

```
Ruijie (config)# interface serial 1/0
Ruijie (config-if)# ip rtp header-connections
```

Related Commands

Command	Description
ip rtp header-compression	Configure RTP packet compressions on the interface.
ip rtp compression-connections	Configure the number of RTP compression connections.
ip tcp compression-connections	Configure the number of TCP compression connections.
show ip rtp header-compression	Show the statistics of IP RTP packet compressions on the interface.

Platform Description

N/A

ip rtp priority

In interface configuration mode, use the **ip rtp priority** command to create an RTP packet priority queue on an interface. Use the **no** form of this command to cancel the RTP packet priority queue.

ip rtp priority *starting-rtp-port-number port-number-range bandwidth*

no ip rtp priority

Parameter Description

Parameter	Description
starting-rtp-port-number	Start port number of matching UDP ports
port-number-range	Port number range of matching UDP ports
bandwidth	Allocated bandwidth (in kbps)

Defaults

By default, there is no RTP packet priority queue.

Command Mode

Interface configuration mode.

Usage Guide

The function of the RTP priority queue (rtpq) is similar to that of llq. That is, each interface has one RTP priority queue, which is used specially for ensuring short-delay transmission of RTP packets and matches UDP packets only in a certain port range.

The traffic of different types in the RTP queue is monitored and is allowed to be sent in the case of non-congestion. In the case of congestion, the sending rate of traffic of different types should be monitored. If it exceeds its bandwidth, the traffic should be discarded.

Each interface has only one RTP priority queue and one llq priority queue, and the priority of the RTP priority queue is higher than that of the llq priority queue.

Caution

To configure priority queue congestion management policies on interfaces, all interfaces of the system need to be configured with the same fast forwarding function. For example, all interfaces are enabled with the fast forwarding function, or all interfaces are disabled with the fast forwarding function. Otherwise, the congestion management policy may fail.

Configuration Examples

The following example shows how to configure the RTP packet priority queue on the sync interface:

```
interface Serial1
service-policy output policy1
ip rtp priority 16384 16383 40
```

Related Commands

Command	Description
service-policy	Configure the policy-map policy associated with an interface.
priority	Configure the number of RTP packet compression connections.
bandwidth (policy-map class)	Configure the traffic bandwidth of cbwfq.
show queue rtp	Display statistics information about IP RTP packet compression.

Platform Description

N/A

ip tcp compression-connections

In interface configuration mode, use the **ip tcp compression-connections** command to configure the number of connections between compression and decompression of TCP packets. Use the **no** form of this command to restore the default value.

ip tcp compression-connections [*number*]

no ip tcp compression-connections

Parameter Description

Parameter	Description
number	Number of connections between packet compression and decompression.

Defaults

The default number of connections are used.

Command Mode

Interface configuration mode.

Usage Guide

The default number of connections are used if the command **ip tcp compression-connections** is not configured. By default, the number for PPP and HDLC is 16 and the number for Frame-relay is 256.

Configuration Examples

The following example shows how to configure connections of TCP packet compression on the sync interface:

```
Ruijie (config)# interface serial 1/0
Ruijie (config-if)# ip tcp header-connections 26
```

Related Commands

Command	Description
ip tcp header-compression	Configure TCP packet compressions on the interface.
ip rtp compression-connections	Configure the number of RTP compression connections.
ip tcp compression-connections	Configure the number of TCP compression connections.

Platform Description

N/A

ip tcp header-compression

In interface configuration mode, use the **ip tcp header-compression** command to apply TCP packet compression on the interface. Use the **no** form of this command to cancel the configuration.

ip tcp header-compression [**passive**]

no ip rtp header-compression

Parameter Description

Parameter	Description
passive	Passive mode for packet compression.

Defaults

No TCP packets are compressed.

Command Mode

Interface configuration mode.

Usage Guide

After **ip rtp header-compression** is configured, the **iphc-format** option and the **ip tcp header-comopression iphc-format** command are automatically added.

Configuration Examples

The following example shows how to configure TCP packet compression on the sync interface:

```
Ruijie (config)# interface serial 1/0
Ruijie (config-if)# ip rtp header-connections
```

Related Commands

Command	Description
ip rtp header-compression	Configure RTP packet compressions on the interface.
ip rtp compression-connections	Configure the number of RTP compression connections.
ip tcp compression-connections	Configure the number of TCP compression connections.
show ip rtp header-compression	Show the statistics of IP RTP packet compressions

	on the interface.

Platform Description N/A

match access-group

Use this command to set the class rule of the class-map to the matching of the ACL, and its **no** form to remove the class match rule.

match access-group *access-list-number*

no match access-group *access-list-number*

Parameter Description

Parameter	Description
access-list-number	Access list number

Defaults By default, no class matching rule is set in the system.

Command Mode Class-map interface configuration mode

Usage Guide Use this command to specify the access list as the class matching rule of the class-map. If the network traffic meets the specified access list, it passes the matching and is added to the corresponding CBWFQ queue.
You can set the match-rule for multiple times on a class-map. However, only the rule set at the last time takes effect. In other words, the current classification rule set will overwrite the previous one.

Configuration Examples In the following example, any network packets meeting the access-list 101 are deemed to meet the class-map class1 and thus are added to the corresponding CBWFQ queue.

```
class-map class1
match access-group 101
```

Related Commands

Command	Description
-	-

Platform Description N/A

match cos

Use this command to set the class rule of the class-map to the cos matching of Ethernet packets, and its **no** form to remove the class match rule.

match cos cos-value [cos-value…]

no match cos cos-value [cos-value…]

Parameter

Parameter	Description

Description	*cos-value*	The matched cos value

Defaults By default, no class matching rule is set in the system.

Command Mode Class-map interface configuration mode

Usage Guide Use this command to specify the Ethernet packet cos vlaue as the class matching rule of the class-map. If the network traffic meets the specified cos value, it passes the matching and is added to the corresponding CBWFQ queue.
You can configure multiple cos values in this command. If there are repeated cos values or the configured code values are not in ascending order, the system performs command adjustment automatically to combine and sort the cos values.

Configuration Examples In the following example, any network packets with the cos value being 3 are deemed to meet class-map class1 and thus are added to the corresponding CBWFQ queue.

```
class-map class1
match cos 3
```

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

Platform Description N/A

match dscp

This command will set the class rule of the class-map to the matching of the DSCP code of the IP TOS field in the IPv4 network packets or of the traffic class field in the IPv6 network packets. Use the **no** form of this command to cancel the class match rule.

match ip dscp dscp-value [dscp-value…]

no match ip dscp dscp-value [dscp-value…]

Parameter Description	Parameter	Description
	dscp-value	Matched dscp value

Defaults By default, no class matching rule is set in the system.

Command Mode Class-map interface configuration mode

Usage Guide Use this command to specify the DSCP code of the IP TOS field in the IPv4 network packets or of the traffic class filed in the IPv6 network packets as the class matching rule of the class-map. If the code value is matched, it passes the class matching and is added to the corresponding CBWFQ queue.
You can configure multiple codes in this command. If the codes configured are duplicated or are not

arranged in the ascending order, the system will automatically adjust the command by combining or sorting the codes.

Note The DSCP of IPv6 takes the first 6 bits in the Traffic Class filed as DHCP value. Thus DSCP=(TC&11111100)>>2. TC value is given by DSCP-to-TC mapping. The detailed relationship is shown below:

DSCP	binary system	000000	000001	…	1111 0	111111
	decimal system	0	1	…	62	63
TC	binary system	00000000 ~00000011	00000100 ~00000111	…	11111000 ~11111011	11111100 ~11111111
	decimal system	0~3	4~7	…	248~251	252~255

When specifying the TC value, run the above algorithm.

Configuration Examples

In this example, if the network packets match any of the DSCP value of 46, 10, and 18, it is deemed that the class-map a1 rule is met.

```
class-map a1
match ip dscp 46 10 18
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A.

match input-interface

Use this command to set an interface to receive packets as a match rule of the class-map. The **no** form of this command removes the settings.

match input-interface *interface-name*

no match input-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Class-map interface configuration mode

Usage Guide

This command is used to set an interface to receive packets as a match rule of the class-map. Packets will be put into the corresponding CBWFQ queue if they arrive at the same interface as the set one.

You can set multiple match rules on a class-map. However, only the last one takes effect. In other words, the newly set match rule will overwrite the previous one.

Configuration Examples

In this example, when packets arrive Fastethernet1, they are considered to match the class-map eth1 rule.

```
class-map eth1
match input-interface fastethernet1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A.

match ip dscp

This command will set the class rule of the class-map to the matching of the DSCP code of the IP TOS field in the network packets, and its **no** form cancels the class match rule.

match ip dscp dscp-value [dscp-value…]

no match ip dscp dscp-value [dscp-value…]

Parameter Description

Parameter	Description
dscp-value	Matched dscp value

Defaults

By default, no class matching rule is set in the system.

Command Mode

Class-map interface configuration mode

Usage Guide

Use this command to specify the DSCP code of the IP TOS field in the network packet as the class matching rule of the class-map. If the code value is matched, it passes the class matching and is added to the corresponding CBWFQ queue.

You can configure multiple codes in this command. If the codes configured are duplicated or are not arranged in the ascending order, the system will automatically adjust the command by combining or sorting the codes.

Configuration Examples

In this example, if the network packets match any of the DSCP value of 46, 10, and 18, it is deemed that the class-map a1 rule is met.

```
class-map a1
match ip dscp 46 10 18
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A.

match ip precedence

This command will set the class rule of the class-map to the matching of the precedence code value of the IP TOS field in the network packets, and its **no** form cancels the class match rule.

match ip precedence precedence-value [precedence-value…]

no match ip precedence precedence-value [precedence-value…]

Parameter Description

Parameter	Description
dscp-value	Matched precedence value

Defaults By default, no class matching rule is set in the system.

Command Mode Class-map interface configuration mode.

Usage Guide Use this command to specify the precedence code of the IP TOS field in the network packet as the class matching rule of the class-map. If the code value is matched, it passes the class matching and is added to the corresponding CBWFQ queue.
You can configure multiple codes in this command. If the codes configured are duplicated or are not arranged in the ascending order, the system will automatically adjust the command by combining or sorting the codes.

Configuration Examples In this example, if the network packets match any of the DSCP value of 0, 2, and 5, it is deemed that the class-map a1 rule is met.

```
class-map a1
match ip precedence 0 2 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

match not

Use this command to set the class rule of the class-map to the matching of no condition of the network packets, and its **no** form to remove this setting.

match not *match-type*

no match not *match-type*

Parameter Description

Parameter	Description
match-type	Class rules to be matched. Rule match is performed based on the *access-group*, *cos*, *input-interface*, *ip dscp*, *ip precedence*, *protocol* parameters.

Defaults By default, no class matching rule is set in the system.

Command Mode Class-map interface configuration mode

Usage Guide If you want to disable the specified class map rule, you can use this command so that no type of network packets matches it.
You can set the match-rule for multiple times on a class-map, and the rule takes effect according to type of the class map.

Configuration Examples In the following example, the class-map class46 is set so that the condition is met for any network data if the DSCP value of the IP TOS domain is not 46.

```
class-map class46
match not ip dscp 46
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

match precedence

This command will set the class rule of the class-map to the matching of the precedence code value of the IP TOS field in the IPv4 network packets or of the traffic class filed in the IPv6 network packets. Use the **no** form of this command to cancel the class match rule.

match ip precedence precedence-value [precedence-value…]

no match ip precedence precedence-value [precedence-value…]

Parameter Description

Parameter	Description
dscp-value	Matched precedence value

Defaults By default, no class matching rule is set in the system.

Command Mode Class-map interface configuration mode.

Usage Guide Use this command to specify the precedence code of the IP TOS field in the IPv4 network packets or of the traffic class filed in the IPv6 network packets as the class matching rule of the class-map. If the

code value is matched, it passes the class matching and is added to the corresponding CBWFQ queue.
You can configure multiple codes in this command. If the codes configured are duplicated or are not arranged in the ascending order, the system will automatically adjust the command by combining or sorting the codes.

Configuration Examples In this example, if the network packets match any of the DSCP value of 0, 2, and 5, it is deemed that the class-map a1 rule is met.

```
class-map a1
match ip precedence 0 2 5
```

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

Platform Description N/A

match protocol

This command will set the class rule of the class-map to match network packet encapsulation protocol type, and its **no** form cancels the class match rule.

match protocol *protocol-name*

no match protocol *protocol-name*

Parameter Description	Parameter	Description
	protocol-name	Name of the encapsulation protocol type (descriptor)

Defaults By default, no class matching rule is set in the system.

Command Mode Class-map interface configuration mode.

Usage Guide Use this command to specify the network packet encapsulation protocol type as the class match rule of the class-map. If the network packet encapsulation protocol type matches the set protocol type, it passes the matching and is added to the corresponding CBWFQ queue.
You can set the match-rule for multiple times on a class-map,and the rule takes effect according to type of the class map. .

Configuration Examples In the following example, if the network packet encapsulation protocol is IP, it is deemed that the class-map class2 rule is met.

```
class-map class2
match protocol ip
```

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

Platform Description N/A

max-reserved-bandwidth

Use this command to allocate bandwidth for the CBWFQ bandwidth on the network interface. The no form of this command restores the system default value.

max-reserved-bandwidth [*percent*]

no max-reserved-bandwidth [*percent*]

Parameter Description

Parameter	Description
percent	Percentage of the total bandwidth of the network interface

Defaults By default, the system allocates 75% of the total available bandwidth to the CBWFQ.

Command Mode Interface configuration mode.

Usage Guide You can use this command to adjust the bandwidth allocated to CBWFQ. However, you must ensure that the allocated bandwidth meets the total bandwidth required by the specified policy map. Otherwise, the CBWFQ fails automatically.

Configuration Examples In the following example, 80% of the total available bandwidth is allocated to the network interface Serial1.

```
interface serial1
max-reserved-bandwidth 80
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

police

Use this command to configure the CAR on the policy-map and apply it on the interface by using the **service-policy** command. The **no** form of this command restores the system default value.

police cir bps{**pir** bps} *burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action* {**violate-action** *violate-action*}

no police cir bps {**pir** bps} *burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action* {**violate-action** *violate-action*}

Parameter Description

Parameter	Description
cir	desired rate upper limit, in bps

pir	desired peak rate of the traffic, in bps
burst-normal burst-max	Size of the token bucket in bytes.
conform-action	Traffic processing policy at rate restriction
exceed-action	Traffic processing policy exceeding the rate restriction
violate-action	Traffic processing policy for the traffic exceeding the second token bucket rate limit when there are two token buckets
action	Processing policy, including the following drop: Drop the packets set-dscp-transmit: Send the packets after setting the field set-prec-transmit: Send the packets after setting the IP precedence field transmit: Send the packets

Defaults By default, no police command is set on the policy-map.

Command Mode Policy-map class interface configuration mode

Usage Guide There are five token bucket algorithms of rate restriction under policy-map. You can select the appropriate token bucket algorithm according to the different configuration.

1.Single token bucket algorithm: If you have not set the violate-action and the value of burst-normal is equal to the burst-max value, the single token bucket algorithm will be used.

2.Lending mode under the single token bucket algorithm: If you have not set the violate-action and the value of burst-normal is less than the burst-max value, the lending mode in the single token bucket algorithm will be used.

3.Single-rate dual token bucket algorithm: If you have set the violate-action but no PIR, the single-rate dual token bucket algorithm will be used.

4.Dual-rate dual token bucket algorithm: If you have set the violate-action and also the PIR, the single-rate dual token bucket algorithm will be used.

If the police command is to be used on the interface, you must configure the service-policy input or service-policy output command on the interface to associate the policy-map with the interface.

Configuration Examples The following example creates a policy map named "policy1" and references a class map in the policy map. The referenced class map "class1" specifies the police rate restriction over the matched packets of the ACL 101 as the matching rule.

```
access-list 101 permit tcp any any eq 2065
!
class-map match-all class1
match access-group 101
!
policy-map policy1
class class1
police cir 80000 2000 2000 conform-action transmit exceed-action drop
violate-action drop
!
interface Serial1/0
```

```
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
service-policy output policy1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

policy-map

Use this command to enter the specified policy map configuration layer. If it is not available, the system will create the policy map. The **no** form of this command deletes the specified policy map.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameter Description	Parameter	Description
	policy-map-name	Name of the rules map, used to identify a policy map in the system.

Defaults By default, no policy map is set in the system.

Command Mode Global configuration mode.

Usage Guide Use this command to enter the policy map configuration layer. On the policy map configuration layer, you can use up to 64 existing class maps on the local device.

After you configure the policy map, you can apply it to the network interface in order to enable CBWFQ. One policy map can be applied to different network interfaces. If the network interface to which the policy map is applied does not meet the total available bandwidth required by the policy map, the CBWFQ cannot be successfully enabled.

Your modification of the policy map will also affect the working performance of CBWFQ on the network interface to which the policy map is applied. If the modified policy map requires a total bandwidth greater than the bandwidth available with the network interface, the CBWFQ on the interface will fail automatically.


Caution

Multiple instances are not supported in a policy map. That is, a policy map only takes effect on a direction of an interface. You need to configure multiple policy maps explicitly to apply them to different directions of an interface or multiple interfaces.


Caution

After ACL stream acceleration is enabled, some streams except quintuples are incorrectly accelerated when you match packets. If you need to match fields like PREC and DSCP, use the included QoS matching rules instead.

Configuration Examples Example 1 creates a policy map named "policy1" and references a class map in the policy map. The referenced class map "class1" specifies the matching of the access list 101 as the matching rule.

The following command creates class map "class1" and defines the class match rule:

```
class-map class1
match access-group 101
```

Example 2: The following command creates the policy map, which references the class map table "class1".

```
policy-map policy1
class class1
bandwidth 2000
queue-limit 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

priority

Use this command to create a IIq low-delay priority queue for the traffic referenced in the policy map, and its **no** form to restore the system default.

priority { *bandwidth-kbps* | **percent** *percent*} {Burst bytes}

no priority

Parameter Description

Parameter	Description
bandwidth-kbps	Allocated bandwidth (in kbps)
percent	Allocated bandwidth percentage (against the total available bandwidth of the network interface) You can allocate bandwidth to the network traffic of the specified type. The system allocates 1% of the total bandwidth to the specified type of network traffic by default.
burst bytes	Packet bytes that may exceed the limit.

Defaults By default, no priority queue is set in the system.

Command Mode Policy-map class interface configuration mode

Usage Guide Ilq is the expansion of the CBWFQ function. It ensures that some packets sensitive to the delay are not only allocated with bandwidth and are sent at low delay.
The Ilq can be understood as PQ+CBWFQ. In other words, there is a strict priority queue, and the packets in the CBWFQ queue will be sent only after the packets in that queue have been sent.
It monitors the different types of traffic of the IIq queue. When this is no congestion, transmission is allowed. In the case of congestion, the rates of different types of traffic are monitored. Those exceeding the bandwidth must be discarded.

Configuration Examples The following example creates a policy map named "policy1" and references a class map in the policy map. The referenced class map "class1" specifies the creation of a priority queue for the matched packets of the ACL 101 as the matching rule.
The following command creates class map "class1" and defines the class match rule:

```
class-map class1
match access-group 101
```

The following command creates the policy map, which references the class map table "class1".

```
policy-map policy1
class class1
priority 2000 25000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

priority-group

In the interface configuration mode, you can use the **priority-group** command to apply the priority queue list to the interface, and the no form of this command to restore the default queue policy of the interface.

priority-group *list-number*

no priority-group

Parameter Description

Parameter	Description
list-number	Priority queue list number, any integer within the 1~16 range

Defaults No priority queue list is allocated.

Command Mode Interface configuration mode

Usage Guide Each interface can be allocated with only one queue list. The priority queue will distinguish the packets according to the priority.
You can use the show queue command to show the status of the current output queue.


Caution

To configure priority queue congestion management policies on interfaces, all interfaces of the system need to be configured with the same fast forwarding function. For example, all interfaces are enabled with the fast forwarding function, or all interfaces are disabled with the fast forwarding function. Otherwise, the congestion management policy may fail.

Configuration Examples The following example shows how to apply priority queue list 10 to sync interface 0:

```
Ruijie(config)# interface serial 0
Ruijie(config-if)# priority-group 10
```

Related Commands

Command	Description
priority-list interface	Create the class rule to allocate packets to the specified priority list according to the interface type.
priority-list protocol	Create the class rule to allocate packets to the specified priority list according to the protocol type.
priority-list queue-limit	Specify the maximum number of packets that a priority queue can accommodate.
show interfaces	Show the interface status.
show queue	Show the queue status of the specified interface.

Platform Description N/A

priority-list default

In the global configuration mode, you can use the **priority-list default** command to allocate a default priority queue to the packets not matching any rule in the custom list. The **no** form of this command allows you to restore the default priority.

priority-list *list-number* **default** { **high** | **medium** | **normal** | **low** }

no priority-list *list-number* **default**

Parameter Description

Parameter	Description
list-number	Priority queue list number, any integer within the 1~16 range.
high | **medium** | **normal** | **low**	Four priorities in the priority queue.

Defaults The default priority is normal.

Command Mode Global configuration mode.

Usage Guide You can configure multiple class rules for each group of the priority queue list. At traffic classification, the system performs matching along the rule chain. If a rule is matched, the packet will be added to the queue of that rule. If the packet does not match any rule, the packet is added to the default queue.

Configuration Examples The following example shows how to set priority queue list 1 and set the priority of the default queue to low:

```
Ruijie(config)#priority-list 1 default low
```

Related Commands

Command	Description
priority-group	Apply the priority list to the interface.
priority-list interface	Allocate packets to the specified priority list according to interface type.
priority-list protocol	Allocate packets to the specified priority list according to the protocol type.
priority-list queue-limit	Specify the maximum number of packets that a priority queue can accommodate.
show queue	Show the queue status on the specified interface.

Platform Description N/A

priority list interface

In the global configuration mode, you can use the **priority-list interface** command to create the class rule, and allocate the packets to the specified priority queue according to the interface type. The **no** form of this command allows you to delete the appropriate class rule.

priority-list *list-number* **interface** *interface-type interface-number* { **high** | **medium** | **normal** | **low** }

no priority-list *list-number* **interface** *interface-type interface-number* { **high** | **medium** | **normal** | **low** }

Parameter Description

Parameter	Description
list-number	Priority queue list number, any integer within the 1~16 range
interface-type	Interface type.
interface-number	Interface number
high | **medium** | **normal** | **low**	Four priorities in the priority queue

Defaults N/A

Command Mode Global configuration mode.

Usage Guide When multiple rules are configured, the RGNO reads the rules according to the specified sequence for comparison. When the first matched item is found, it stops lookup and adds the data packets to the appropriate queue.

Configuration Examples The following example shows how to set priority list 3 so that the packets from sync interface 1 are allocated to the medium priority queue:

```
Ruijie(config)# priority-list 3 interface serial 1 medium
```

This command only defines the rule. To put the rule into effect, you must use the priority-group command.

Related Commands

Command	Description
priority-group	Apply the priority list to the interface.
priority-list default	Allocate the packets not matching any rules of the custom queue to a default priority queue.
priority-list protocol	Allocate packets to the specified priority list according to the protocol type
priority-list queue-limit	Specify the maximum number of packets that a priority queue can accommodate.
show queue	Show the queue status on the specified interface.

Platform Description N/A

priority-list protocol

In the global configuration mode, you can use the **priority-list protocol** command to create the class rule, and allocate the packets to the specified priority queue according to the protocol type. The **no** form of this command allows you to delete the appropriate class rule.

priority-list *list-number* **protocol** *protocol-name* { **high** | **medium** | **normal** | **low** } [*queue-keyword keyword-value*]

no priority-list *list-number* **protocol** [*protocol-name* { **high** | **medium** | **normal** | **low** } [*queue-keyword keyword-value*]]

Parameter Description

Parameter	Description
list-number	Priority queue list number, any integer within the 1~16 range
protocol-name	Protocol type: arp, bridge, compressedtcp, ip, llc2 and pad.
high | medium | normal | low	Four priorities in the priority queue.
queue-keyword keyword-value	Some options of various protocols

queue- keyword	keyword- value	Meaning
Null	Null	Any packets belonging to this protocol can enter the specified queue
fragments	Null	Any fragmented IP packets can enter the specified queue
list	list- number	Any packets matching the access list list-number can enter the specified queue
Lt	byte-count	The packets whose length is less than the value set by the byte-count command can enter the specified value
Gt	byte-count	The packets whose length is higher than the value set by the byte-count command can enter the specified value
tcp	port	The IP packets whose source or destination TCP port number is port enter the specified queue
udp	port	The IP packets whose source or destination UDP port number is port enter the specified queue

Defaults No queue priority rule.

Command Mode Global configuration mode.

Usage Guide When multiple rules are configured, the RGNO reads the rules according to the specified sequence for comparison. When the first matched item is found, it stops lookup and adds the data packets to the appropriate queue.

Configuration Examples Example 1 shows how to set priority list 2 so that all the packets whose protocol type is IP are allocated to the high priority queue:

```
Ruijie(config)# priority-list 2 protocol ip high
```

Example 2 shows how to set priority queue list 7 so that all the packets matching IP ACL 101 are allocated to the high priority queue:

```
Ruijie(config)priority-list 7 protocol ip high list 101
```

Example 3 shows how to set priority queue list 6 so that all the packets with a length greater than 250 bytes are allocated to the medium priority queue:

```
Ruijie(config)# priority-list 6 protocol ip medium gt 250
```

Example 4 shows how to set priority queue list 11 so that all the packets with a length smaller than 250 bytes are allocated to the medium priority queue:

```
Ruijie(config)# priority-list 11 protocol ip medium lt 250
```

Related Commands

Command	Description
priority-group	Apply the priority list to the interface.
priority-list default	Allocate the packets not matching any rules of the custom queue to a default priority queue.
priority-list interface	Allocate packets to the specified priority list according to the interface type.
priority-list queue-limit	Specify the maximum number of packets that a priority queue can accommodate.
show queue	Show the queue status of the specified interface.

Platform Description N/A.

priority-list queue-limit

In the global configuration mode, you can use the **priority-list queue-limit** command to specify the maximum number of packets that each priority queue can accommodate. The **no** form of this command allows you to restore the default value.

priority-list list-number **queue-limit** [**high-limit** [**medium-limit** [**normal-limit** [**low-limit**]]]]

no priority-list *list-number* **queue-limit**

Parameter Description

Parameter	Description
list-number	Priority queue list number, any integer within the 1~16 range
high-limit medium-limit normal-limit low-limit	Priority queue length, where 0 means no restriction on the length of the queue. The default values are shown in the following table:

Queue	Default length
high-limit	0
medium-limit	40
normal-limit	60
low-limit	80

Defaults See the parameter description for the default values of various queue lengths

Command Mode Global configuration mode.

Usage Guide If the priority queue overflows, the new packets will be discarded.

Configuration Examples The following example shows how to set the lengths of the queues in priority queue list 3:

```
Ruijie(config)# priority-list 3 queue-limit 10 40 60 80
```

Related Commands

Command	Description
priority-group	Apply the priority list to the interface
priority-list default	Allocate the packets not matching any rules of the custom queue to the default priority queue
priority-list interface	Create the class rule to allocate packets to the specified priority list according to the interface type
priority-list protocol	Allocate packets to the specified priority list according to the protocol type
show queue	Show the queue status on the specified interface

Platform Description N/A

queue-limit

Use this command to set the queue depth for the CBWFQ of the class map referenced in the policy mapping table. The **no** form of this command restores the settings to the default value.

queue-limit number-of-packets

no queue-limit

Parameter Description

Parameter	Description
number-of-packets	Depth of the CBWFQ queue of the referenced class map, that is, the maximum number of network packets that can be accommodated concurrently

Defaults By default, the depth of the CBWFQ queue of the referenced class map is 64. In other words, a maximum of 64 network packets can be accommodated concurrently.

Command Mode Policy-map class interface configuration mode.

Usage Guide

The RGOS uses the Tail_Drop method to handle the congestion when the CBWFQ queue is full. In other words, after the number of network packets in the CBWFQ queue reaches the set queue depth, the packets that attempt to join the CBWFQ queue will be discarded.

You can use this command to set the depth of the CBWFA queue corresponding to the referenced class map, and this will also affect the performance of the CBWFA on the related network interface.

The configuration of queue depth requires consideration of network requirements. If forwarded data is delay-sensitive, you can decrease the queue depth to reduce the forwarding delay. If data burst is serious or there are many small-sized packets, you can increase the queue depth to enhance the system's buffering capability.

Do not set the queue depth too small, or the bandwidth guarantee function may not work properly.

If data burst is serious or there are many small-sized packets, queue bandwidth cannot be guaranteed. In this case, it is necessary to increase the queue depth to enhance the buffering capability.

Configuration Examples

In the following example, the policy map "policy11" references the class map "acl203" and sets the corresponding CBWFA queue length to 40.

```
policy-map policy11
class acl203
bandwidth 2000
queue-limit 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

queue-list default

In the global configuration mode, you can use the **queue-list default** command to allocate a custom queue to the packets not matching any rule in the custom list. The **no** form of this command allows you to restore the default value.

queue-list list-number **default** queue-number

no queue-list *list-number* **default**

Parameter Description

Parameter	Description
list-number	Queue list number, any integer within the 1~16 range
queue-number	Queue list number, any integer within the 0~16 range

Defaults

The default queue number of the custom queue is 1.

Command Mode

Global configuration mode.

Usage Guide You can configure multiple class rules for each group of the custom queue list. In traffic classification, the RGOS performs matching along the rule chain. If a rule is matched, the packet will be added to the queue of that rule. If the packet does not match any rule, the packet is added to the default queue.
Queue 0 is the system queue, the first queue that is cleared.
You can use the show queue command to show the status of the current output queue.

Configuration Examples The following example shows how to specify the default queue of first group of the custom queue list:

```
Ruijie(config)# queue-list 1 default 1
```

Related Commands

Command	Description
custom-queue-list	Apply the custom queue list to the interface.
queue-list interface	Allocate packets to the specified custom queue according to interface type.
queue-list protocol	Allocate packets to the specified custom queue according to protocol type.
queue-list queue byte-count	Specify the number of bytes that can be sent continuously while polling the queue.
queue-list queue limit	Specify the maximum number of packets that a custom queue can accommodate.

Platform Description N/A

queue-list interface

In the global configuration mode, use the **queue-list interface** command to create an interface-based class rule, enter the interface type according to the packets, and allocate packets to the specified custom queue. Use the “no” form of this command to delete the classification rule.

queue-list *list-number* **interface** *interface-type interface-number queue-number*

no queue-list *list-number* **interface** *interface-type interface-number queue-number*

Parameter Description

Parameter	Description
list-number	Queue list number, any integer within the 1~16 range
interface-type	Interface type.
interface-number	Interface number
queue-number	Queue list number, any integer within the 0~16 range

Defaults N/A

Command Mode Global configuration mode.

Usage Guide When multiple rules are configured, the system reads the rules according to the specified sequence

for comparison. When the first matched item is found, it stops lookup and adds the data packets to the appropriate queue.

Configuration Examples The following example shows how to create a rule that allocates the packets from Serial 1 to custom queue 3:

```
Ruijie(config)# queue-list 1 interface serial 1 3
```

Related Commands

Command	Description
custom-queue-list	Apply the custom queue list to the interface.
queue-list default	Allocate the packets not matching any rules of the custom queue list to a default queue.
queue-list protocol	Allocate packets to the specified custom queue according to protocol type.
queue-list queue byte-count	Specify the number of bytes that can be sent continuously while polling the queue.
queue-list queue limit	Specify the maximum number of packets that a custom queue can accommodate.
show queue	Show the queue status on the specified interface.

Platform Description N/A

queue-list protocol

In the global configuration mode, you can use the **queue-list protocol** command to create the protocol-based queue classification rule that allocates the packets to the specified custom queue according to the protocol type of the packets. The **no** form of this command allows you to delete the appropriate rule.

queue-list *list-number* **protocol** *protocol-name queue-number* [*queue-keyword keyword-value*]

no queue-list *list-number* **protocol** [*protocol-name queue-number* [*queue-keyword keyword-value*]]

Parameter	Description
list-number	Queue list number, any integer within the 1~16 range
protocol-name	protocol type, the ip is usually used
queue-number	queue list number, any integer within the 0~16 range
queue-keyword keyword-value	some options of various protocols

Parameter Description

queue- keyword	Keyword- value	Meaning
Null	Null	Any packets belonging to this protocol can enter the specified queue
fragments	Null	Any fragmented IP packets can enter the specified queue
list	list-number	Any packets matching the access list list-number can enter the specified queue
lt	byte-count	The packets whose length is less than the value set by the byte-count command can enter the specified value

gt	byte-count	The packets whose length is higher than the value set by the byte-count command can enter the specified value
tcp	Port	The IP packets whose source or destination TCP port number is port enter the specified queue
udp	Port	The IP packets whose source or destination UDP port number is port enter the specified queue

Defaults No priority rule is defined

Command Mode Global configuration mode

When multiple rules are configured, the RGOS reads the rules according to the specified sequence for comparison. When the first matched item is found, it stops lookup and adds the data packets to the appropriate queue.

Usage Guide


Caution

When protocol rules specify fragments policy, express forwarding must be disabled on all interfaces since the current software version does not support the rules to link with the fragments policy in the express forwarding mode.

Configuration Examples

Example 1 shows how to set custom list 4 to allocate the Telnet packets to queue 2:

```
Ruijie(config)#queue-list 4 protocol ip 2 tcp 23
```

Example 2 shows how to set custom list 1 to allocate the UDP domain name service packets to queue 3:

```
Ruijie(config)#queue-list 1 protocol ip 3 udp 53
```

Example 3 shows how to set custom list 2 to allocate the packets matching ACL 100 to queue 1:

```
Ruijie(config)#queue-list 2 protocol ip 1 list 100
```

Related Commands

Command	Description
custom-queue-list	Apply the custom queue list to the interface.
queue-list default	Allocate the packets not matching any rules of the custom queue list to a default queue.
queue-list queue byte-count	Specify the number of bytes that can be sent continuously while polling the queue.
queue-list queue limit	Specify the maximum number of packets that a custom queue can accommodate.
show queue	Show the queue status on the specified interface.

Platform Description N/A

queue-list queue byte-count

In the global configuration mode, you can use the **queue-list queue byte-count** command to specify the number of packet types that can be sent continuously at each polling. The **no** form of this command restores the default value.

queue-list list-number **queue** *queue-number* **byte-count** *byte-count-number*

no queue-list list-number **queue** *queue-number* **byte-count** *byte-count-number*

Parameter Description

Parameter	Description
list-number	Queue list number, any integer within the 1~16 range.
queue-number	Queue number, any integer within the 0~16 range.
byte-count-number	Number of bytes of the packets that can be sent continuously at each polling in the queue, within the range of 1~16777215.

Defaults The *byte-count* is 1500 bytes

Command Mode Global configuration mode.

Usage Guide

The bytes that a queue can deliver must be configured according to the traffic condition of each queue, and it should be avoided to configure excess byte count for a low traffic queue, or else the current queue may be scheduled all the time, thus affecting the processing of other queues.

Configuration Examples The following example specifies that 1400 packet types can be sent continuously for queue 5 of custom list 2:

```
Ruijie(config)# queue-list 2 queue 5 byte-count 1400
```

Related Commands

Command	Description
custom-queue-list	Apply the custom queue list to the interface.
queue-list default	Allocate the packets not matching any rules of the custom queue list to a default queue.
queue-list interface	Allocate packets to the specified custom queue according to interface type.
queue-list protocol	Allocate packets to the specified custom queue according to protocol type.
queue-list queue limit	Specify the maximum number of packets that a custom queue can accommodate.
show queue	Show the queue status on the specified interface.

Platform Description N/A

queue-list queue limit

In the global configuration mode, you can use the **queue-list queue limit** command to specify the maximum number of packets that each custom queue can accommodate. The **no** form of this command allows you to restore the default value.

queue-list *list-number* **queue** *queue-number* **limit** *limit-number*

no queue-list *list-number* **queue** *queue-number* **limit** *limit-number*

Parameter Description

Parameter	Description
list-number	Queue list number, any integer within the 1~16 range
queue-number	Queue number, any integer within the 0~16 range
limit-number	Maximum number of packets that the queue can accommodate; within the range of 1~32767, defaulted to 20.

Defaults 20 packets

Command Mode Global configuration mode.

Usage Guide If the queue is full, the new packets will be discarded.

Configuration Examples **The following example shows how to specify 40 packets as the length of custom queue 5:**

```
Ruijie(config)# queue-list 2 queue 5 limit 40
```

Related Commands

Command	Description
custom-queue-list	Apply the custom queue list to the interface.
queue-list default	Allocate the packets not matching any rules of the custom queue list to a default queue.
queue-list interface	Allocate packets to the specified custom queue according to interface type.
queue-list protocol	Allocate packets to the specified custom queue according to protocol type.
queue-list queue byte-count	Specify the number of bytes that can be sent continuously while polling the queue.
show queue	Show the queue status on the specified interface.

Platform Description N/A

random-detect

Use this command to enable the interface congestion avoidance policy on the network interface, which is precedence classification based on IP packets. The no form of this command restores the system default value.

random-detect

no random-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the system has not applied any interface congestion avoidance policy on the network interface.

Command Mode

Interface configuration mode or Policy-map class interface configuration mode.

Usage Guide

WRED avoids the global synchronization of TCP by randomly discarding packets — when the packets of a TCP connection are discarded and the transmission speed is reduced, other TCP connections still maintain a high transmission speed. This way, there are always some TCP connections that transmit packets at a high speed at any time, for higher utilization of the line bandwidth.

By default, the congestion avoidance policy without any parameter is enabled on the interface. The congestion avoidance policy is the precedence classification based on IP packets, into up to 8 types of traffic.

To configure avoidance management policy on the interface, all interfaces of the system must have the same express forwarding configuration (all enabling or disabling express forwarding), or else the congestion avoidance policy may fail.

Configuration Examples

The following example configures the default congestion avoidance policy on the outgoing interface.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
random-detect
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

random-detect dscp

Use this command to configure the threshold parameters for the congestion avoidance policy based on DSCP class packet flows. This no form of this command allows you to restore the default value.

random-detect dscp *dscp-value min-threshold max-threshold mark-prob-denominator*

no random-detect dscp *dscp-value min-threshold max-threshold mark-prob-denominator*

Parameter Description

Parameter	Description
dscp-value	dscp value for traffic classification

min-threshold	Minimum discard threshold, for which the default value varies with each type of traffic
max-threshold	Maximum discard threshold, for which the default value varies with each type of traffic
mark-prob-denominator	Discard probability, defaulted to 10, that is, 1/10; the higher this value, the lower the discard probability

Defaults By default, the threshold parameters of each congestion avoidance policy based on dscp packet flows can be shown by using the show queue interface command.

Command Mode Interface configuration mode or Policy-map class interface configuration mode

Usage Guide After congestion avoidance based on dscp packet classification is configured, each type of dscp traffic has its default discard threshold and probability. You can use the random-detect dscp command to re-define the discard threshold and probability for each type of dscp packet flow.

Configuration Examples The following example configures congestion avoidance based on DSCP packet classification on the outgoing interface and sets anew its discard threshold and probability to each type of packet whose DSCP value is af11, af21, af31, and af41.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
random-detect dscp-based
random-detect dscp af11 5 100 10
random-detect dscp af21 10 100 10
random-detect dscp af31 20 100 10
random-detect dscp af41 30 100 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A.

random-detect dscp-based

Use this command to enable the interface congestion avoidance policy on the network interface, which is DSCP classification based on IP packets. The no form of this command restores the system default value.

random-detect dscp-based

no random-detect dscp-based

Parameter Description

Parameter	Description
N/A	N/A

Defaults	By default, the system has not applied any interface congestion avoidance policy on the network interface.
Command Mode	Interface configuration mode or Policy-map class interface configuration mode.
Usage Guide	Use this command to enable the congestion avoidance policy based on the DSCP field on the interface. The congestion avoidance policy is the DSCP classification based on IP packets, into up to 64 types of traffic. After the policy is enabled, the DSCP value has its default discard threshold and probability, and the threshold parameters can be shown by using the show queue interface command.

Configuration Examples	The following example configures the congestion avoidance policy based on IP DSCP classification on the outgoing interface.
	`interface Serial1/0`
	`ip address 192.168.20.3 255.255.255.0`
	`encapsulation ppp`
	`random-detect dscp-based`

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

Platform Description	N/A

random-detect prec-based

Use this command to enable the interface congestion avoidance policy on the network interface, which is precedence classification based on IP packets. The no form of this command restores the system default value.

random-detect prec-based

no random-detect prec-based

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

Defaults	By default, the system has not applied any interface congestion avoidance policy on the network interface.
Command Mode	Interface configuration mode or Policy-map class interface configuration mode

Usage Guide WRED avoids the global synchronization of TCP by randomly discarding packets——when the packets of a TCP connection are discarded and the transmission speed is reduced, other TCP connections still maintain a high transmission speed. This way, there are always some TCP connections that transmit packets at a high speed at any time, for higher utilization of the line bandwidth.

By default, the congestion avoidance policy without any parameter is enabled on the interface. The congestion avoidance policy is the precedence classification based on IP packets, into up to 8 types of traffic.

Configuration Examples The following example configures the ip precedence-based congestion avoidance policy on the outgoing interface.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
random-detect prec-based
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

random-detect precedence

Use this command to configure the threshold parameters for the congestion avoidance policy based on precedence class packet flows. This **no** form of this command allows you to restore the default value.

random-detect precedence *precedence-value min-threshold max-threshold mark-prob-denominator*

no random-detect precedence *precedence-value min-threshold max-threshold mark-prob-denominator*

Parameter Description

Parameter	Description
prec-value: precedence	Precedence dscp value for traffic classification
min-threshold	Minimum discard threshold, for which the default value varies with each type of traffic
max-threshold	Maximum discard threshold, for which the default value varies with each type of traffic
mark-prob-denominator	Discard probability, defaulted to 10, that is, 1/10; the higher this value, the lower the discard probability

Defaults By default, the threshold parameters of each congestion avoidance policy based on precedence packet flows can be shown by using the show queue interface command.

Command Mode Interface configuration mode or Policy-map class interface configuration mode

Usage Guide After congestion avoidance based on precedence packet classification is configured, each type of

precedence traffic has its default discard threshold and probability. You can use the random-detect precedence command to re-define the discard threshold and probability for each type of precedence packet flow.

Configuration Examples The following example configures congestion avoidance based on precedence packet classification on the outgoing interface and sets anew its discard threshold and probability to each type of packet whose precedence value is 1, 2, 3 and 4.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
random-detect prec-base
random-detect precedence 1 5 100 10
random-detect precedence 2 10 100 10
random-detect precedence 3 20 100 10
random-detect precedence 4 30 100 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

random-detect exponential-weighting-constant

Use this command to configure the weighting factor of congestion avoidance. Use the **no** form of this command restores the system default value.

random-detect exponential-weighting-constant *exponential-value*

no random-detect exponential-weighting-constant *exponential-value*

Parameter Description

Parameter	Description
exponential-value	Weighting factor, defaulted to 9; the lower this value, the higher the discard probability; the higher this value, the lower the discard probability.

Defaults By default, the weighting factor of congestion avoidance is 9.

Command Mode Interface configuration mode or Policy-map class interface configuration mode

Usage Guide When the weighting factor is changed, every type of traffic will be affected. The default weighting factor is 9; the lower this value, the higher the discard probability; the higher this value, the lower the discard probability.

Configuration Examples Example 1 configures the congestion avoidance policy based on precedence packet classification on the outgoing interface, and sets the weighting factor to 15.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
random-detect prec-base
random-detect exponential-weighting-constant 15
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A.

rate-limit

This command enables the CAR on the express forwarding interface. The no form of this command restores the system default value.

rate-limit {**input** | **output**} {*bps* | **access-group** *acl-index* | | **dscp** *dscp-value* } *burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

no rate-limit {**input** | **output**} [**access-group** *acl-index* | **dscp** *dscp-value*] *bps burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

Parameter Description

Parameter	Description
input|output	Input/output traffic to restrict
bps	Desired rate upper limit, in bps
burst-normal burst-max	This is the size of the token bucket in bytes.
conform-action	traffic processing policy at rate restriction
exceed-action	traffic processing policy exceeding the rate restriction
action	Processing policy, including the following
Continue:	Continue to match the next policy:
drop	Drop the packets
set-dscp-continue	After the packet dscp field is set, the packet continues to match the next policy
set-dscp-transmit	Send the packets after setting the field
set-prec-continue	After the ip precedence field is set, the packet continues to match the next policy
set-prec-transmit	Send the packets after setting the ip precedence field
transmit	Send the packets

Defaults By default, the system has not applied any interface rate restriction on the express forwarding

interface.

Command Mode Interface configuration mode

Usage Guide The CAR uses the token bucket algorithm. You can set the capacity of the token bucket. If the packet meets the pre-set match rule, it enters the token bucket for processing. If the packet does not meet the match rule, it is continuously sent. For the packets undergoing the token bucket processing, the packets are continuously sent if there are sufficient tokens, and are discarded if there are no sufficient tokens.

Ruijie series support at least 1K restricted flows and CAR-ACL binding. Consequently, you can enable traffic classification and rate limit at the same time.

Caution When IPSec encryption is enabled on the interface, the traffic monitoring (CAR) won't be able to support the change of CAR policies, such as set-dscp-continue, set-prec-continue, set-dscp-transmit, and set-prec-transmit. If multiple ACL CARs are configured and each flow matches one ACL, all matched flows take effect, If a flow matches ACL1 and ACL2, ACL1 takes effect. If a flow matches the same ACL rules with different actions, all ACL rules take effect.

Caution The priority of access-group, dscp and default decreases, and set-continue only takes effect on rate limiting of the same priority. It is not executed across different priorities.

Caution The size of token bucket must be configured according to the potential burst of network traffic. If there are such bursting services as video or file transfer on the network, the size of token bucket must be increased in order to enhance the burst tolerance capacity of QoS. It is generally suggested to configure the token bucket to support at least 200ms buffering capacity, namely (CIR/8)*200ms.

Configuration Examples Example 1 configures CAR on the outgoing interface.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
rate-limit output 300000 3000 3000 conform-action  transmit exceed-action
drop
```

Example 2 enforces CAR over the traffic meeting the ACL on the outgoing interface.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
```

```
encapsulation ppp
rate-limit output access-group 101 256000 5000 5000 conform-action  transmit
exceed-action  set-dscp-transmit 46
rate-limit output access-group 102 200000 3000 3000 conform-action  transmit
exceed-action  set-prec-transmit 5
rate-limit output access-group 103 128000 3000 3000 conform-action  transmit
exceed-action  set-prec-transmit 1
```

Example 3 enforces CAR over the traffic meeting the DSCP on the outgoing interface.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
rate-limit  output  dscp  46  256000  5000  5000  conform-action   transmit
exceed-action  set-dscp-transmit 46
rate-limit  output  dscp  10  200000  3000  3000  conform-action   transmit
exceed-action  set-prec-transmit 5
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

service-policy

Use this command to apply the policy map of the specified name and enable the CBWFQ function on the network interface. The no form of this command restores the system default value.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Parameter Description	**Parameter**	**Description**
	policy-map-name	Name of the policy map used

Defaults By default, the system has not applied any policy map on the network interface.

Command Mode Interface configuration mode

Usage Guide When you apply the policy map on the network interface, you must ensure that the bandwidth of the network interface allocated to the CBWFQ must meet the total bandwidth required by the specified policy map. Otherwise, the policy map cannot be successfully applied.


Caution

To configure policy map on the interface, all interfaces of the system must have the same express forwarding configuration (all enabling or disabling express forwarding), or else the functions corresponding to policy map may fail, such as CBWFQ, police,

etc.

To configure ingress policy map and associate with egress policy map with shape and red features, express forwarding must be disabled on the interface. In the current release, in express forwarding mode, the interface cannot be applied with ingress policy map or associated with egress policy map with shape and red features.

Examples In the following example, the policy map named "policy9" is applied on network interface Serial1 and the CBWFQ is enabled.

```
interface serial1
service-policy output policy9
```

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

Platform Description N/A

set cos

Use this command to set the cos value for the traffic specific to the class mapping table called in the rule mapping table. The **no** form of this command restores the system default value.

set cos { *cos-value* | { **precedence | dscp** [**table** *table-map-name*] } }

no set cos { *cos-value* | { **precedence | dscp** [**table** *table-map-name*] } }

Parameter Description	**Parameter**	**Description**
	cos-value	The cos value to be set
	table-map-name	The name of the table-map to be called

Defaults By default, the system does not apply this command in the rule mapping table.

Command Mode Policy-map class interface configuration mode

Usage Guide No special requirements.

Configuration Examples **In the following example, the rule mapping table named "policy1" matches the packets of the class mapping table acl203, with all cos values set to 4.**

```
policy-map policy1
class acl203
set ip cos 4
```

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

Platform Description N/A.

set ip dscp

Use this command to set the DSCP code for the IP TOS field of the class map referenced in the policy mapping table. The no form of this command restores the system default value.

set ip dscp *dscp-value*

no set ip dscp *dscp-value*

Parameter Description

Parameter	Description
dscp-value	dscp value to be set

Defaults By default, the system does not apply this command on the policy map.

Command Mode Policy-map class interface configuration mode

Usage Guide No special requirements

Configuration Examples The following example sets the IP DSCD code to 46 for the packets matching the class map acl203 on the policy map "policy1".

```
policy-map policy1
class acl203
set ip dscp 46
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A.

set ip precedence

Use this command to set the precedence code for the IP TOS field of the class map referenced in the policy mapping table. The no form of this command restores the system default value.

set ip precedence *precedence-value*

no set ip precedence *precedence-value*

set ip precedence *dscp-value*

no Set ip precedence *dscp-value*

Parameter

Parameter	Description

Description	*precedence-value*	Precedence value to set

Defaults By default, the system does not apply this command on the policy map.

Command Mode Policy-map class interface configuration mode

Usage Guide No special requirements

Configuration Examples TExample 1 sets the IP precedence value to 5 for the packets matching the class map acl203 on the policy map "policy1".

```
policy-map policy1
class acl203
set ip precedence 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

set precedence

Use this command to set the precedence code for the IPv4 TOS field and IPv6 traffic class field of the class map referenced in the policy mapping table. The **no** form of this command restores the system default value.

set precedence *precedence-value*

no set precedence *precedence-value*

Parameter Description

Parameter	Description
precedence-value	Precedence value to be set

Default configuration By default, the system does not apply this command on the policy map.

Command Mode Policy-map class interface configuration mode

Usage Guide No special requirements

Configuration Examples The following example sets both the IPv4 and IPV6 precedence code to 5 for the packets matching the class map acl203 on the policy map "policy1":

```
policy-map policy11
class acl203
set precedence 5
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

traffic-shape group

This command enables the rate traffic shaping GTS function on the network interface. The no form of this command restores the system default value.

traffic-shape group *access-list bit-rate* [*burst-size* [*excess-burst-size*]] [*buffer-limit*]

no traffic-shape group *access-list*

Parameter Description

Parameter	Description
access-list	Access list for matching the traffic
bit-rate	Desired rate upper limit to shape, in bps. The maximum value is 1000000000 (1 Gbps).
burst-size	Maximum burst packets of each interval, in bits
excess-burst-size	Burst packets of the first interval, in bits
buffer-limit	Size of the GTS buffer queue, defaulted to 1000

Defaults By default, the system has not applied any interface rate traffic shaping on the network interface.

Command Mode Interface configuration mode

Usage Guide The Generic Traffic Shaping (GTS) allows you to shape the packet traffic irregular or not meeting the preset traffic feature to ensure bandwidth matching between the upstream and downstream. The GTS is performed through the packet buffer and token bucket. When the packet traffic is sent at too high a speed, the packets are first buffered and then evenly sent under the control of the token bucket.

This command performs traffic shaping to the data traffic undergoing the standard or extended Access Control List (ACL).

On the interface, the traffic-shape group command and traffic-shape rate command are mutually exclusive. In other words, if you have configured the traffic-shape group command, you cannot configure the traffic-shape rate command. It is also the case the other way around.


Caution

With the ACL classification associated with the shape function on the interface, fast forwarding function must be disabled. The current software version does not support the traffic shaping function associated with ACL classification in the express forwarding mode.

Configuration Examples The following example enforces GTS over the traffic meeting the ACL on the outgoing interface.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
traffic-shape group 101 256000 10240 10240 1000
traffic-shape group 102 200000 8000 8000 1000
traffic-shape group 103 128000 10240 10240 1000
traffic-shape group 104 64000 12800 12800 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

traffic-shape rate

This command enables the rate traffic shaping GTS function on the network interface to perform interface traffic shaping to all the IP traffic of the entire interface. The no form of this command restores the system default value.

traffic-shape rate *bit-rate* [*burst-size* [*excess-burst-size*]] [*buffer-limit*]

no traffic-shape rate

Parameter Description

Parameter	Description
bit-rate	Desired rate upper limit to shape, in bps. The maximum value is 1000000000 (1Gbps).
burst-size	Maximum burst packets of each interval, in bits.
excess-burst-size	Burst packets of the first interval, in bits.
buffer-limit	Size of the GTS buffer queue, defaulted to 1000.

Defaults By default, the system has not applied any interface rate traffic shaping on the network interface.

Command Mode Interface configuration mode

Usage Guide The Generic Traffic Shaping (GTS) allows you to shape the packet traffic irregular or not meeting the preset traffic feature to ensure bandwidth matching between the upstream and downstream. The GTS is performed through the packet buffer and token bucket. When the packet traffic is sent at too high a speed, the packets are first buffered and then evenly sent under the control of the token bucket.

This command performs traffic shaping to all the traffics passing the physical interface.

On the interface, the traffic-shape group command and traffic-shape rate command are mutually exclusive. In other words, if you have configured the traffic-shape group command, you cannot configure the traffic-shape rate command. It is also the case the other way around.


Caution

The traffic shaping policy handled by the system will function on the interface. When GTS has been configured for the interface, all related subinterfaces of this interface must enable GTS, or else the traffic forwarding will become uneven on related subinterfaces.


Caution

After traffic shaping is enabled on the interface, the burst traffic must be the integral multiple of the data transmitted at 10ms under traffic-shaping rate, or else the system will round off the burst traffic configuration parameters according to the data transmitted at 10ms under traffic-shaping rate, so that the parameters can become valid.


Caution

The size of token bucket must be configured according to the potential burst of network traffic. If there are such bursting services as video or file transfer on the network, the size of token bucket must be increased in order to enhance the burst tolerance capacity of QoS. It is generally suggested to configure the token bucket to support at least 200ms buffering capacity, namely (CIR/8)*200ms.


Caution

GTS cannot know the line expenses on ATM interfaces, so the rate limiting is not accurate. The passed traffic is higher than the theoretical calculation. If you need to limit rates accurately on ATM interfaces, use rate limiting commands such as CBR and UBR provided by ATM.


Caution

GTS needs to calculate interframe gap and CRC when limiting rates, so the method for calculating the GTS rate limiting is as follows:

The number of passed packets (pps) = Value of GTS rate limit (bps) / [(packet length + interframe gap + CRC) x 8], and floor the result for accuracy.
(2) Rate at the receiving end = PPS x Size of received packets (byte) x 8

Configuration Examples

Example 1 enforces GTS over all the traffics on the outgoing interface.

```
interface Serial1/0
ip address 192.168.20.3 255.255.255.0
encapsulation ppp
traffic-shape rate 256000 10240 10240 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Showing Related Commands

show class-map

Use this command to show the related information on the class-map.

show class-map [*class-map-name*]

Parameter description

Parameter	Description
class-map-name	Name of the class map

Default N/A

Command mode Privileged EXEC mode.

Usage guide You can use this command to show the related information of the class-map on the system.

Configuration Examples Example 1 shows the information of all the class maps on the system.

```
Ruijie# show class-map
Class Map class-default
Match any
Class Map class6
Match protocol arp
Class Map class5
Match input-interface FastEthernet0
Class Map class4
Match none
Class Map class1
Match access-group 101
Class Map class2
Match access-group 102
Class Map class3
Match access-group 103
```

You can see that this command shows the name of all class maps the class match rules on the system.

Example 2 shows the information of the class map named “class1”.

```
Ruijie# show class-map class1
Class Map class1
Match access-group 101
```

You can see that this command shows the class match rule of the class map with the specified name.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip rtp header-compression

Use this command to show the compression and decompression of RTP packets on the specifiefd interface in privileged EXEC mode.

show ip rtp header-compression *interface-name interface-number*

Parameter description

Parameter	Description
interface-name	Name of the interface
interface-number	Number of the interface

Default N/A

Command mode Privileged EXEC mode.

Usage guide You can use this command to show the related information of the compression and decompression of RTP packets on the specified network interface.

Configuration Examples Example 1 shows the information of RTP packet compression and decompression on Serial 1/0.

```
Ruijie# show ip rtp header-compression serial 1/0
RTP/UDP/IP header compression statistics:
Interface serial 1/0: active on
Rcvd: 407 total, 406 compressed,0 errors
0 dropped, 406 buffer copies,0 buffer failures
Sent: 406 totol, 405 compressed,
14716 bytes saved, 8494 bytes sent
2.73 efficiency improvement factor
Connect: 256 rx slots, 256 tx slots, 0 long searches, 1 misses 99%
hit ratio, five minute miss rate 0 misses/sec, 0 max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip tcp header-compression

Use this command to show the compression and decompression of TCP packets on the specifiefd interface in privileged EXEC mode.

show ip tcp header-compression *interface-name interface-number*

Parameter description

Parameter	Description
interface-name	Name of the interface
interface-number	Number of the interface

Default N/A

Command mode Privileged EXEC mode.

Usage guide You can use this command to show the related information of the compression and decompression of TCP packets on the specified network interface.

Configuration Examples Example 1 shows the information of TCP packet compression and decompression on Serial 1/0.

```
Ruijie# show ip tcp header-compression serial 1/0
TCP/IP header compression statistics:
Interface serial 1/0: active on
Rcvd: 14 total, 12 compressed,0 errors
0 dropped, 12 buffer copies,0 buffer failures
Sent: 24 totol, 18 compressed,
607 bytes saved, 815 bytes sent
1.74 efficiency improvement factor
Connect: 256 rx slots, 256 tx slots, 0 long searches, 2 misses 91%
hit ratio, five minute miss rate 0 misses/sec, 0 max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show policy-map

Use this command to show the related information of the policy-map on the system.

show policy-map [**name** *policy-map-name* [**class** *class-map-name*] | **interface** *interface-name*]

Parameter Description

Parameter	Description
policy-map-name	Name of the policy map;
class-map-name	Name of the class map;
interface-name	Name of network interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the related information of the policy-map on the system.

Note RSR series routers support the show policy-map interface command to view the statistical information about express forwarding rule mapping table.

Configuration Examples The following example shows the information of all the policy maps on the system.
Assuming the following configuration:

```
policy-map 1
 class 1
  bandwidth 100
 class 2
 bandwidth percent 5
 class 3
priority 100 2500
class 4
priority percent 5 1250000
 class 5
set ip dscp 1
 class 6
police cir 100000 2000 2000 conform-action transmit exceed-action drop
policy-map 2
 class 1
bandwidth 2000
policy-map 3
 class 2
 set ip dscp 2
Ruijie# show policy-map
Policy Map 1
Class 1
 Bandwidth 100 (kbps) Max Thresh 64 (packets)
 Class 2
 Bandwidth 5 (%) Max Thresh 64 (packets)
Class 3
Strict Priority
 Bandwidth 100 (kbps) Max Thresh 64 (packets), Burst 2500 (Bytes)
Class 4
Strict Priority
Bandwidth 5 (%) Max Thresh 64 (packets), Burst 1250000 (Bytes)
Class 5
set ip dscp 1
     mark action order 0
   Class 6
     police cir 100000 2000 2000 conform-action transmit exceed-action drop
     police action order 0
 Policy Map 2
   Class 1
     Bandwidth 2000 (kbps) Max Thresh 64 (packets)

 Policy Map 3
   Class 2
     set ip dscp 2
     mark action order 0
```

You can see that this command shows the information of all the policy maps on the system: All referenced class map names, bandwidth allocation and CBWFQ queue depth of the class maps.

The following example shows the information of the rule map applied on the Serial 0 interface.

Configure service-policy output 1 on serial 0.

```
Ruijie# show policy-map  interface serial 0
   Class 1
   Class 2
   Class 3
   Class 4
   Class 5
     set ip dscp 1
     mark count 0

   Class 6
     current token tbf: TC_ONETBF
     params:  100000 bps, 2000 limit, 2000 extended limit , 0 pir
     conformed 0 packets, 0 bytes; action: transmit 0
     exceeded 0 packets, 0 bytes; action: drop 0
     violated 0 packets, 0 bytes; action: none 0
     cbucket 4000, cbs 4000; ebucket 0 ebs 0

Serial 5/0  output :
   Weighted Fair Queueing
   Class 1
     Output Queue: queue_num 265
       Bandwidth 100 (kbps) Packets Matched 0 Sended 0 Max Thresh 64 (packets)
       (discards/tail drops) 0/0 , weight 16384
   Class 2
     Output Queue: queue_num 266
       Bandwidth 5 (%) Packets Matched 0 Sended 0 Max Thresh 64 (packets)
       (discards/tail drops) 0/0 , weight 819
   Class 3
     Output Queue: queue_num 267
     Strict Priority
     Bandwidth 100 (kbps) Max Thresh 64 (packets), Burst 2500 (Bytes)
     cir 100000 bucket 0, cburst 0 cpkt 0, eburst 0 epkt 0, nbytes 0 npkt 0
       (discards/tail drops) 0/0 , weight 4096
   Class 4
     Output Queue: queue_num 268
     Strict Priority
     Bandwidth 5 (%) Max Thresh 64 (packets), Burst 1250000 (Bytes)
     cir 50000000 bucket 0, cburst 0 cpkt 0, eburst 0 epkt 0, nbytes 0 npkt
0
       (discards/tail drops) 0/0 , weight 4096
   Class 5
```

```
    Output Queue: queue_num 269
      (discards/tail drops) 0/0 , weight 4096
  Class 6
    Output Queue: queue_num 270
      (discards/tail drops) 0/0 , weight 4096
QoS Ref Policy-map information
Policy-map Output: 1
  Class 1
    Bandwidth 100 kbps
      conformed 0 packets, 0 bytes
      exceeded 0 packets, 0 bytes
      violated 0 packets, 0 bytes
      cbucket 128000, cbs 128000; ebucket 0 ebs 128000
  Class 2
    Bandwidth 5%
      conformed 0 packets, 0 bytes
      exceeded 0 packets, 0 bytes
      violated 0 packets, 0 bytes
      cbucket 128000, cbs 128000; ebucket 0 ebs 128000
  Class 3
    Strict Priority, Bandwidth 100 kbps
      conformed 0 packets, 0 bytes
      exceeded 0 packets, 0 bytes
      violated 0 packets, 0 bytes
      cbucket 128000, cbs 128000; ebucket 0 ebs 128000
  Class 4
    Strict Priority, Bandwidth 5%
      conformed 0 packets, 0 bytes
      exceeded 0 packets, 0 bytes
      violated 0 packets, 0 bytes
      cbucket 128000, cbs 128000; ebucket 0 ebs 128000
  Class 5
    set ip dscp 1
      mark count 0
  Class 6
    policy
      current token tbf: TC_ONETBF
      params:  100000 bps, 2000 limit, 2000 extended limit , 0 pir
     conformed 0 packets, 0 bytes; action: transmit 0
      exceeded 0 packets, 0 bytes; action: drop 0
      violated 0 packets, 0 bytes; action: none 0
      cbucket 4000, cbs 4000; ebucket 0 ebs 0
```

You can see that this command shows the information of the policy map applied on the specified network interface on the system: All referenced class map names, the code of CBWFQ session sequence of the class map, bandwidth allocation and CBWFQ queue depth of the class map.

This command also displays related token bucket parameters of express forwarding. For class maps configured with policy, bandwidth and priority, there is a corresponding token bucket in the express forwarding to color packets based on rates specified by class maps. The detailed parameters of the token buckets are described below:

```
   Class 1 (matched class map)
     Bandwidth 100 kbps (policy type corresponding to the class map, 100 kbps
of CBWFQ in this example)
       conformed 0 packets (number of packets that colored green), 0 bytes
(number of bytes of packets colored green)
       exceeded 0 packets (number of packets that colored yellow), 0 bytes
(number of bytes of packets colored yellow)
       violated 0 packets (number of packets that colored red), 0 bytes (number
of bytes of packets colored red)
       cbucket 128000 (size of the token bucket corresponding to the current
green packets), cbs 128000 (capacity of the token bucket of green packets);
ebucket 0 (size of the token bucket corresponding to the current yellow
packets), ebs 128000 (capacity of the token bucket of yellow packets).

Single token bucket algorithm: cbs = burst – normal + burst - max, ebs = 0.
Single rate double token buckets: cbs = burst – normal, ebs = burst - max
Double rate double token buckets: cbs = burst – normal, ebs = burst - max
```

The following example shows the information of the policy map named “policy1”.

```
Ruijie# show policy-map name policy1
Policy Map 1
   Class 1
     Bandwidth 100 (kbps) Max Thresh 64 (packets)
   Class 2
     Bandwidth 5 (%) Max Thresh 64 (packets)
   Class 3
     Strict Priority
     Bandwidth 100 (kbps) Max Thresh 64 (packets), Burst 2500 (Bytes)
   Class 4
     Strict Priority
     Bandwidth 5 (%) Max Thresh 64 (packets), Burst 1250000 (Bytes)
   Class 5
     set ip dscp 1
     mark action order 0

   Class 6
     police cir 100000 2000 2000 conform-action transmit exceed-action drop
     police action order 0
```

You can see that this command shows the information of the policy map of the specified name on the system: All referenced class map names, bandwidth allocation and CBWFQ queue depth of the

class maps.

The following example shows the information of the class map “class2” referenced by the policy map named “policy1”.

```
Ruijie# show policy-map name policy1 class class2
   Class 2
     Bandwidth 5 (%) Max Thresh 64 (packets)
```

You can see that this command shows the information of the class map of the specified name referenced in the policy map of the specified name: All referenced class map names, bandwidth allocation and CBWFQ queue depth of the class maps.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A.

show queue

In the privileged mode, you can use the **show queue** command show the queue status of the specified interface.

show queue interface interface-name interface-number [queue-number]

show queue {*cq* | *pq* | *wfq*}

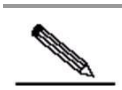
Parameter Description

Parameter	Description
interface-name	Interface name
interface-number	Interface number
queue-number	Queue number
cq	CQ queue parameter of the CQ interface
pq	PQ queue parameter of the PQ interface
wfq	WFQ queue parameter of the WFQ interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the related information of the QoS queue on the specified network interface on the system.



Note

You can use the show queue interface command to view the statistical information about cbwfq/cq/pq/rtpq/wfq queue interface express forwarding for the RSR series router. The express forwarding statistics is marked with “Qos Ref queue information”.

Configuration Examples

Assuming the following parameters configured on the interface gigabitEthernet 0/0:

```
ip rtp priority 2000 2000 2000
 ip address 200.1.1.1 255.255.255.0
 traffic-shape rate 80000 8000 8000 1000
 service-policy output 1
duplex auto
speed auto
```

The following example shows the related information of the QoS queue .

```
Ruijie# show queue interface gigabitEthernet 0/0
 Queueing strategy: cb weighted fair
 Output queue: 0/300/128/0 (size/max total/threshold/drops)
  cb queue_num  0/0 (active/max active)
  wfq queue_num  0/0 (active/max active)
    Reserved queue_num 6/6 (allocated/max allocated)
    Llq is open
```

You can see that this command shows the QoS queue information on the specified network interface: reception queue statistics, transmission queue (QoS) policy and transmission queue statistics. The statistics of the transmission queue vary with the QoS policy (FIFO, PQ, CQ, WFQ or CBWFQ).

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show rate-limit

Use this command to show the related information of the rate-limit command statistics on the interface.

show rate-limit [*interface*]

Parameter Description

Parameter	Description
interface	Interface for which the rate-limit command is configured

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide You can use this command to show the related information of rate-limit on the system.

Note RSR series routers support the show rate-limit interface command to view the statistical information about the monitored traffic on the express forwarding interface.

Configuration Examples The following example shows the information of all the class maps on the system.

```
Ruijie# show rate-limit
serial 1/0
Output
matches access-group 101
  params:  256000 bps, 3000 limit, 3000 extended limit
  conformed 0 packets, 0 bytes; action: transmit
  exceeded 0 packets, 0 bytes; action: drop
  cbucket 6000, cbs 6000; ebucket 0 ebs 0
```

The above information shows:

```
serial 1/0 (interface of the configuration command)
Output (configured direction)
matches access-group 101 ( matched ACL number)
params:  256000 bps (committed rate per second), 3000 limit (normal burst
flow), 3000 extended limit (abnormal burst flow)
conformed 0 packets, 0 bytes (actual flow of normal burst so far); action:
transmit (action taken in normal burst)
exceeded 0 packets, 0 bytes (actual flow of abnormal burst so far); action:
drop (action taken in abnormal burst)
Cbucket 6000 (depth of the current normal burst bucket), cbs 6000 (maximum
depth of the normal burst bucket); ebucket 0 (depth of the current abnormal
burst bucket), ebs 0 (maximum depth of the abnormal burst bucket).

Single token bucket algorithm: cbs = burst – normal + burst - max, ebs = 0.
Single rate double token buckets: cbs = burst – normal, ebs = burst - max
Double rate double token buckets: cbs = burst – normal, ebs = burst - max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show traffic-shape

Use this command to show the related information of the configured policy by the traffic-shape command on the interface of the system.

show traffic-shape [*interface*]

Parameter Description	Parameter	Description
	interface	Interface configured with the traffic-shape

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the related information of the traffic-shape on the system.

Configuration Examples The following example shows the information of all the interfaces configured with traffic-shape on the system.

```
Ruijie# show traffic-shape
Interface serial 1/0
Access Target  Byte   Sustain  Excess   Interval Increment   Adapt
VC  List  Rate  Limit   bits/int   bits/int  (ms)  (bytes)  Active
-   -    300000    2250    9000     9000    30      1125     -
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A.

show traffic-shape queue

Use this command to show the information of the related buffer queues of the configured policy by the traffic-shape command on the interface of the system.

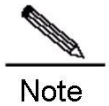
show traffic-shape queue [*interface*]

Parameter Description	Parameter	Description
	interface	Interface configured with the traffic-shape

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the information of the related buffer queues of the traffic-shape on the system.


Note

You can use the show queue interface command to view the statistical information about express forwarding traffic shaping interface token for the RSR series router. The express forwarding statistics is marked with “Qos Ref queue information”.

Configuration Examples The following example shows the information of the buffer queues of ll the interfaces configured with traffic-shape on the system.

```
Ruijie# show traffic-shape queue
Traffic queued in shaping queue on serial 1/0
Traffic shape group: null
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Output queue num: 0/0 (now/max)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show traffic-shape statistics

Use this command to show the packet statistics of the configured policy of traffic-shape on the interface of the system.

show traffic-shape statistics [*interface*]

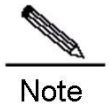
Parameter Description

Parameter	Description
interface	Interface configured with the traffic-shape

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the information of the packet statistics of the traffic-shape on the system.



Note

You can use the show queue interface command to view the statistical information about express forwarding traffic shaping interface token for the RSR series router. The express forwarding statistics is marked with “Qos Ref queue information”.

Configuration Examples The following example shows the information of the packet statistics configured with traffic-shape on the system.

```
Ruijie# show traffic-shape statistics
Interface serial 1/0
Acc. Queue   Packets   Bytes   Packets   Bytes      Shaping
List  Depth  Delayed   Delayed   Active
-     0          0     0      0     0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

HQOS Commands

8021p-inbound

This command is used to set the CoS-based traffic policy for 802.1P inbound traffic in the diffserv domain. The no form of this command is used to restore the default policy.

8021p-inbound *cos-value* **phb** *service-class color*

no 8021p-inbound *cos-value* **phb** *service-class color*

Parameter Description

Parameter	Description
cos-value	The 802.1P priority field of Ethernet packets, ranging from 0 to 7
service-class	Class of service mapped to a traffic class
color	Packet color corresponding to a traffic class

Defaults

By default, the 802.1P inbound traffic policy exists after the diffserv domain is created.

Command Mode

diffserv domain configuration mode

Usage Guide

You can use this command to change the mapping between a 802.1P priority and a CoS and discard priority. Combining the outbound traffic policy, you can enable a simple traffic policy. Hierarchical QoS (HQoS) supports eight classes of service, namely, cs7, cs6, ef, af1, af2, af3, af4, and be, which are described as follows:

Class of Service		Description
CS7		It is used for in-band control messages, with the highest priority.
CS6		It is used for protocol packets on the control plane, such as routing protocol packets and BFD packets.
EF (Expedited Forwarding)		It is used for services that require delay, jitter, and packet loss rate guarantees, such as VoIP and TDM.
AF4	Assured Forwarding	Forwarding these services is assured when they do not exceed the maximum allowed bandwidth. Once they exceed the bandwidth, they will be discarded according to their priorities. These services fall into four categories, each allocated different bandwidth.
AF3		
AF2		
AF1		
BE (Best Effort)		It is used for services not sensitive to delay, jitter, and packet loss, such as Internet services like Web and FTP.

HQoS supports green, yellow, and red, and supports configuration of different packet drop policies for these three colors using WRED.

Configuration Examples

Example 1: Configure the packets with 802.1p priority of 3 to the CoS of EF and green color.

```
Ruijie(config)#diffserv domain 8021p
Ruijie(config-diffserv-domain)#8021p-inbound 3 phb ef green
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8021p-outbound

This command is used to set the CoS- and color-based traffic policy for 802.1P outbound traffic in the diffserv domain. The **no** form of this command is used to restore the default policy.

8021p-outbound *service-class color* **map** *cos-value*

no 8021p-outbound *service-class color* **map** *cos-value*

Parameter Description

Parameter	Description
cos-value	The 802.1P priority field value of Ethernet packets, ranging from 0 to 7
service-class	Class of service mapped to a traffic class
color	Color corresponding to a traffic class

Defaults **By default, the 802.1P outbound traffic policy exists after the diffserv domain is created.**

Command Mode diffserv domain configuration mode

Usage Guide

You can use this command to change the mapping between a class of service and a 802.1P priority. Combining the inbound traffic policy, you can enable a simple traffic policy.

Hierarchical QoS (HQoS) supports eight classes of service, namely, cs7, cs6, ef, af1, af2, af3, af4, and be, which are described as follows:

Class of Service		Description
CS7		It is used for in-band control messages, with the highest priority.
CS6		It is used for protocol packets on the control plane, such as routing protocol packets and BFD packets.
EF (Expedited Forwarding)		It is used for services that require delay, jitter, and packet loss rate guarantees, such as VoIP and TDM.
AF4	Assured Forwarding	Forwarding these services is assured when they do not exceed the maximum allowed bandwidth. Once they exceed the bandwidth, they will be discarded according to their priorities. These services fall into four categories, each allocated different bandwidth.
AF3		
AF2		
AF1		
BE (Best Effort)		It is used for services not sensitive to delay, jitter, and packet loss, such as Internet services like Web and FTP.

HQoS supports green, yellow, and red, and supports configuration of different packet drop policies for these three colors using WRED.

Configuration Examples

Example 1: Map the packets with the CoS of EF and green color to the 802.1p priority of 3.

```
Ruijie(config)# diffserv domain 8021p
Ruijie(config-diffserv-domain)#8021p-outbound ef green map 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

cir

This command is used to set the committed information rate (CIR) for queues. The **no** form of this command is used to cancel the traffic rate limit for queues.

cir *cir-value* [**pir** *pir-value]*

no cir *cir-value* [**pir** *pir-value]*

Parameter Description

Parameter	Description
cir-value	The upper limit of the CIR for queues, ranging from 1 to 10000000 (Kbit/s)
pir-value	The upper limit of the peak information rate (PIR) for queues, ranging from 1 to 10000000 (Kbit/s)

Defaults

The rate is limited to 0 by default.

Command Mode

use-queue interface configuration mode

Usage Guide

If only the CIR is configured, the single-rate token bucket is used to limit the rate; if the PIR is configured, the dual-rate token bucket is used to limit the rate.

Configuration Examples

Example 1: Use the dual-rate token bucket to limit the rate for the queue uq1.

```
Ruijie(config)#user-queue uq1 inbound
Ruijie(confg-user-queue)#cir 10000 pir 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

classifier

This command is used to specify the traffic behavior for a traffic classifier. The **no** form of this command is used to cancel the association between a traffic classifier and traffic behavior.

classifier *classifier-name* **behavior** *behavior-name* [**precedence** *precedence-value]*

no classifier *classifier-name* **behavior** *behavior-name* [**precedence** precedence-value]

Parameter Description

Parameter	Description
classifier-name	The name of a traffic classifier
behavior-name	The name of a traffic behavior
precedence-value	The precedence value of a traffic policy. 1000 precedence values are supported, a smaller value representing a higher priority.

Defaults	The system does not assign a traffic behavior to any traffic classifier by default.
Command Mode	traffic policy configuration mode
Usage Guide	The traffic classifier and traffic behavior used in a classifier must exist in the device; otherwise, you cannot use them in the classifier. Multiple traffic classifiers and traffic behaviors can be associated in a traffic policy, and precedence values are given to differentiate traffic policies, a smaller value representing a higher priority. The first-match-quit mode is adopted for the traffic classifiers and traffic behaviors in a traffic policy, which means that once the first traffic classifier/behavior is matched, the traffic policy is quitted. If no precedence values are assigned to traffic policies, the traffic policies are prioritized according to their configuration order.

Configuration Examples	Example 1: The traffic classifier rule tcr1 is associated with traffic behavior rule tbr1 in traffic policy tpr1. In this way, actions in tbr1 are implemented for the network traffic that matches tcr1, and the priority of the policy is 10.
	`Ruijie(config)#traffic policy tpr1`
	`Ruijie(config-traffic-policy)#classifier tcr1 behavior tbr1 precedence 10`

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

clear port-queue

This command is used to clear the port-queue statistics for an interface.

clear port-queue statistics interface *interface-name*

Parameter Description	**Parameter**	**Description**
	interface-name	The name of the interface

Defaults N/A

Command Mode Privileged mode

Usage Guide This command is used to clear the port-queue statistics for an outbound interface in HQoS only.

Configuration Examples Example 1: Clear the port-queue statistics for the interface GE 0/0/1.

```
Ruijie#clear port-queue statistics interface gigabitethernet 0/1/1
```

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

Platform Description N/A

clear user-group-queue

This command is used to clear statistics of a user group queue for a device.

clear user-group-queue statistics *user-group-queue-name* { **outbound** | **inbound }**

Parameter Description

Parameter	Description
user-group-queue-name	The name of a user group queue
inbound | *outbound*	Direction of a user group queue, inbound or outbound

Command Mode Privileged mode

Usage Guide This command is used to clear statistics of a user group queue for a device, whose ID should be specified.
The device ID can be calculated using the slot and subslot: devid=slot*3+subslot. You can use the show version slot command to check the slot and subslot information in the slot field.

Configuration Examples Example 1: Clear statistics of the outbound user group queue gq1 for device 6.

```
Ruijie# clear user-group-queue  statistics gq1 outbound  devid 6
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear user-queue

This command is used to clear statistics of a user queue for a device.

clear user-queue statistics *user-queue-name* { **outbound | inbound** }

Parameter Description

Parameter	Description
user-queue-name	The name of a user queue
inbound | *outbound*	Direction of a user queue, inbound or outbound

Defaults N/A

Command Mode Privileged mode

Usage Guide This command is used to clear statistics of a user queue for a device, whose ID should be specified.
The device ID can be calculated using the slot and subslot: devid=slot*3+subslot. You can use the show version slot command to check the slot and subslot information in the slot field.

Configuration Example 1: Clear statistics of the outbound user queue uq1 for device 6.

Examples

```
Ruijie# clear user-queue statistics uq1  outbound  devid 6
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

color

This command is used to set thresholds for three colors of packets for congestion avoidance. The **no** form of this command is used to restore default thresholds for the three colors of packets for congestion avoidance.

color {**green** | **yellow** | **red**} **low-limit** *low-limit-percent* **high-limit** *high-limit- percent* **discard-percent** *discard-percent-value*

no color {green | yellow | red} low-limit *low-limit-percent* **high-limit** *high-limit- percent* **discard-percent** *discard-percent-value*

Parameter Description

Parameter	Description
green | *yellow* | *red*	Packet color
low-limit-percent	Queue depth low-limit percentage
high-limit-percent	Queue depth high-limit percentage
discard-percent-value	The discard percentage value, which defaults to 100

Defaults

The default packet drop thresholds of WRED are as follows:

Packet Color	Queue Depth Low Limit Percentage (%)	Queue Depth High Limit Percentage (%)	Discard Percentage (%)
green	**70**	**100**	**100**
yellow	**60**	**90**	**100**
red	**50**	**80**	**100**

Command Mode

WRED configuration mode

Usage Guide

Each WRED has default packet drop thresholds and discard percentages. You can use the color command to reset the drop thresholds and discard percentages. The high-limit/low-limit and discard percentage for red packets can be set to the smallest, those for yellow packets can be set the medium, and those for green packets can be set to the largest.

Configuration Examples

Example 1: The WRED template wt1 defines packet drop thresholds and discard percentages for three colors of packets.

```
Ruijie(config)#wred wt1
Ruijie(config-wred)#color green low-limit 40 high-limit 60 discard-percent 10
Ruijie(config-wred)#color yellow low-limit 30 high-limit 50 discard-percent
10
Ruijie(config-wred)#color red low-limit 20 high-limit 40 discard-percent 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

diffserv domain

This command is used to enter the configuration layer of a diffserv domain of a specific name. If the specified diffserv domain does not exist, the system creates a diffserv domain with the name. The **no** form of the command is used to delete the diffserv domain of the name from the system.

diffserv domain {*diffserv-name* | **default**}

no diffserv domain *diffserv-name*

Parameter Description

Parameter	Description
diffserv-name	The name of the diffserv domain

Defaults

The system creates a default diffserv domain by default.

Command Mode

Global configuration mode

Usage Guide

You can use this command to specify a diffserv domain, which supports the mapping between MPLS EXP, IP DSCP, 802.1p cos and class of service, discard priority. A diffserv domain maintains the following six mapping relationships:

1. 8021p-inbound

2. 8021p-outbound

3. ip-dscp-inbound

4. ip-dscp-outbound

5. mpls-exp-inbound

6. mpls-exp-outbound

After a diffserv domain is created, the default mapping policy is used for the initialization. The following table lists the default mapping policy.

DSCP	Service	Color	DSCP	Service	Color
00	BE	Green	32	AF4	Green
01	BE	Green	33	BE	Green
02	BE	Green	34	AF4	Green
03	BE	Green	35	BE	Green
04	BE	Green	36	AF4	Yellow
05	BE	Green	37	BE	Green
06	BE	Green	38	AF4	Red
07	BE	Green	39	BE	Green
08	AF1	Green	40	EF	Green
09	BE	Green	41	BE	Green
10	AF1	Green	42	BE	Green
11	BE	Green	43	BE	Green
12	AF1	Yellow	44	BE	Green
13	BE	Green	45	BE	Green
14	AF1	Red	46	EF	Green
15	BE	Green	47	BE	Green
16	AF2	Green	48	CS6	Green
17	BE	Green	49	BE	Green
18	AF2	Green	50	BE	Green
19	BE	Green	51	BE	Green
20	AF2	Yellow	52	BE	Green
21	BE	Green	53	BE	Green
22	AF2	Red	54	BE	Green
23	BE	Green	55	BE	Green
24	AF3	Green	56	CS7	Green
25	BE	Green	57	BE	Green
26	AF3	Green	58	BE	Green
27	BE	Green	59	BE	Green
28	AF3	Yellow	60	BE	Green
29	BE	Green	61	BE	Green
30	AF3	Red	62	BE	Green
31	BE	Green	63	BE	Green

Mapping relationship between the default DSCP and Cos service types.

Service	Color	DSCP
BE	Green, Yellow, Red	0
AF1	Green	10
AF1	Yellow	12
AF1	Red	14
AF2	Green	18
AF2	Yellow	20
AF2	Red	22
AF3	Green	26

AF3	Yellow	28
AF3	Red	30
AF4	Green	34
AF4	Yellow	36
AF4	Red	38
EF	Green, Yellow, Red	46
CS6	Green, Yellow, Red	48
CS7	Green, Yellow, Red	56

Default mapping relationship between the default Qos and DSCP service types.

EXP	Service	Color
00	BE	Green
01	AF1	Green
02	AF2	Green
03	AF3	Green
04	AF5	Green
05	EF	Green
06	CS6	Green
07	CS7	Green

Default mapping relationship between the default EXP and QoS service types.

Service	Color	EXP
BE	Green, Yellow, Red	0
AF1	Green, Yellow, Red	1
AF2	Green, Yellow, Red	2
AF3	Green, Yellow, Red	3
AF4	Green, Yellow, Red	4
EF	Green, Yellow, Red	5
CS6	Green, Yellow, Red	6
CS7	Green, Yellow, Red	7

Default mapping relationship between the default QoS and EXP service types.

Cos	Service	Color
00	BE	Green
01	BE	Green
02	AF2	Green
03	AF2	Green
04	AF4	Green
05	AF4	Green
06	CS6	Green
07	CS7	Green

Default mapping relationship between the Cos and QoS service types.

Service	Color	cos

BE	Green, Yellow, Red	0
AF1	Green, Yellow, Red	1
AF2	Green, Yellow, Red	2
AF3	Green, Yellow, Red	3
AF4	Green, Yellow, Red	4
EF	Green, Yellow, Red	5
CS6	Green, Yellow, Red	6
CS7	Green, Yellow, Red	7

Default Mapping relationship between the QoS and Cos service types.

Configuration Examples

Example 1: Create the diffserv domain ipdscp for the MPLS ingress PE.

```
Ruijie(config)#diffserv domain ipdscp
Ruijie(config-diffserv-domain)#exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

flow-mapping

This command is used to enter the configuration layer of a flow-queue mapping template of a specific name. If the flow-queue mapping template of the name does not exist, the system creates the template with the name. The **no** form of the command is used to delete the flow-queue mapping template of the name from the system.

flow-mapping *flow-mapping-name*

no flow-mapping *flow-mapping-name*

Parameter Description

Parameter	Description
flow-mapping-name	The name of the flow-queue mapping template

Defaults

No flow-queue mapping template exists by default.

Command Mode

Global configuration mode

Usage Guide

You can use the flow-mapping command to create a flow-queue mapping template of the specific name and enter the flow-queue mapping template configuration mode. You can configure eight mappings between flow-queue priorities and port-queue priorities.

Configuration Example

Example 1: Establish mapping in the flow-queue mapping template between packets whose flow-queue priority is af1 and packets whose port-queue priority is ef.

```
Ruijie(config)#flow-mapping fmt1
Ruijie(config-flow-mapping)# map flow-queue af1 to port-queue ef
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

flow-mapping (user-queue)

The **flow-mapping** command is used under a user-queue to apply the specified flow-queue mapping template to a user queue, so that flow queues in the user queue are mapped to port queues according to template parameters. The **no** form of this command is used to delete the mapping between flow queues and port queues.

flow-mapping *flow-mapping-name*

no flow-mapping *flow-mapping-name*

Parameter Description	Parameter	Description
	flow-mapping-name	The name of the flow-queue mapping template

Defaults No flow-queue mapping rules are associated by default.

Command Mode use-queue interface configuration mode

Usage Guide The flow-queue mapping template must exist in the device; otherwise, you cannot apply the template to the user queue.
When no flow-queue mapping template is configured for the user queue, one-to-one mapping is established between flow-queue priorities and port-queue priorities.

Configuration Examples Example 1: Apply flow-queue mapping template fmt1 to user queue uq1.

```
Ruijie(config)#user-queue uq1 inbound
Ruijie(config-user-queue)#flow-mapping fmt1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

flow-queue

This command is used to enter the configuration layer of a flow-queue template of a specific name. If the flow-queue template of the name does not exist, the system creates the template with the name. The **no** form of the command is used to delete the flow-queue template of the name from the system.

flow-queue *flow-queue-name*

no flow-queue *flow-queue-name*

Parameter Description	Parameter	Description
	flow-queue-name	**The name of the flow-queue template**

Defaults A default flow-queue template exists in the system by default.

Command Mode Global configuration mode

Usage Guide You can use the flow-queue command to create a flow-queue template of the specific name and enter the flow-queue interface configuration mode. You can configure scheduling parameters for eight flow-queue priorities on the flow-queue interface.

Configuration Examples Example 1: Configure scheduling parameters for different flow-queue priorities in the flow-queue template.

```
Ruijie(config)#flow-queue fqt1
Ruijie(config-flow-queue)# queue be lpq
Ruijie(config-flow-queue)# queue af1 wfq weight 10 shaping 100000 wred wt1
Ruijie(config-flow-queue)# queue cs7 pq shaping wred wt1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

flow-queue (user-queue)

The **flow-queue** command is used under a user-queue to apply the specified flow-queue template to a user queue, so that flow queues in the user queue are scheduled according to template parameters. The **no** form of this command is used the restore the default flow-queue parameters.

flow-queue *flow-queue-template-name*

no flow-queue *flow-queue-template-name*

Parameter Description	Parameter	Description
	flow-queue-template-name	The name of the flow-queue template

Defaults By default, the user queue is associated with the default flow-queue template.

Command Mode use-queue interface configuration mode

Usage Guide The flow-queue template must exist in the device; otherwise, you cannot apply the template to the user queue.
If no flow-queue template is associated, the user queue is scheduled with the CoS of BE.

Configuration Examples

Example 1: Apply the flow-queue template fqt1 to user queue uq1.

```
Ruijie(config)#user-queue uq1 inbound
Ruijie(config-user-queue)#flow-queue fqt1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

if-match acl

This command is used to set the classification rule for IPv4 packets in a traffic classifier to matching an ACL. The **no** form of this command is used to cancel the configuration.

if-match acl *acl-number*

no if-match acl *acl-number*

Parameter Description

Parameter	Description
acl-number	ACL number

Defaults

No classification rule is configured in the system by default.

Command Mode

traffic classifier interface configuration mode

Usage Guide

You can use this command to specify an ACL as the classification rule of a traffic classifier. If data flows match the specified ACL, they meet the classification rule of the classifier.
The classification rule only applies to IPv4 packets.

Configuration Examples

Example 1: Configure all packets that match ACL 101 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match acl 101
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

if-match any

This command is used to set the classification rule of a traffic classifier to matching any IPv4 packets. The **no** form of this command is used to cancel the configuration.

if-match any

no if-match any

Parameter Description

Parameter	Description
N/A	N/A

Defaults No classification rule is configured in the system by default.

Command Mode traffic classifier interface configuration mode

Usage Guide You can use this command to set any IPv4 packets to match the traffic classifier.
The classification rule only applies to IPv4 packets.

Configuration Examples Example 1: Configure any packets to match traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match any
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

if-match cos

This command is used to set the classification rule of a traffic classifier to matching the 802.1P packet CoS. The **no** form of this command is used to cancel the configuration.

if-match cos *cos-value*

no if-match cos *cos-value*

Parameter Description

Parameter	Description
cos-value	The CoS value to be matched

Defaults No classification rule is configured in the system by default.

Command Mode traffic classifier interface configuration mode

Usage Guide You can use this command to specify the CoS value of Ethernet packets as the classification rule of a traffic classifier. If data flows match the CoS value, they meet the classification rule of the classifier.
The classification rule only applies to 802.1P packets.

Configuration Examples Example 1: Configure packets whose CoS value is 1 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match cos 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

if-match destination-mac

This command is used to set the classification rule of a traffic classifier to matching the destination MAC address of the Ethernet packets. The **no** form of this command is used to cancel the configuration.

if-match destination-mac *mac-address*

no if-match destination-mac *mac-address*

Parameter Description	Parameter	Description
	mac-address	Ethernet MAC address

Defaults No classification rule is configured in the system by default.

Command Mode traffic classifier interface configuration mode

Usage Guide You can use this command to specify the Ethernet destination MAC address of packets as the classification rule of a traffic classifier. If data flows match the MAC address, they meet the classification rule of the classifier.
The classification rule only applies to Ethernet packets.

Configuration Examples Example 1: Configure the packets that match the destination MAC address 00d0.f822.33ac to match traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match destination-mac 00d0.f822.33ac
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

if-match dscp

This command is used to set the classification rule of a traffic classifier to matching the DSCP value in the tos field in IPv4 packets. The **no** form of this command is used to cancel the configuration.

if-match dscp *dscp-value*

no if-match dscp *dscp-value*

Parameter Description

Parameter	Description
dscp-value	The DSCP value to be matched

Defaults No classification rule is configured in the system by default.

Command Mode traffic classifier interface configuration mode

Usage Guide You can use this command to specify the DSCP value in the ip tos field in packets as the classification rule of a traffic classifier. If data flows match the DSCP value, they meet the classification rule of the classifier.
The classification rule only applies to IPv4 packets.

Configuration Examples Example 1: Configure packets whose DSCP value is 10 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match dscp 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

if-match ip-precedence

This command is used to set the classification rule of a traffic classifier to matching the precedence value in the tos field in IPv4 packets. The **no** form of this command is used to cancel the configuration.

if-match ip-precedence *precedence-value*

no if-match ip-precedence *precedence-value*

Parameter Description

Parameter	Description
precedence-value	The precedence value to be matched

Defaults No classification rule is configured in the system by default.

Command Mode traffic classifier interface configuration mode

Usage Guide You can use this command to specify the precedence value in the ip tos field in packets as the classification rule of a traffic classifier. If data flows match the precedence value, they meet the classification rule of the classifier.

The classification rule only applies to IPv4 packets.

Configuration Examples

Example 1: Configure packets whose precedence value is 1 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match ip-precedence 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

if-match ipv6 acl

This command is used to set the classification rule for IPv6 packets in a traffic classifier to matching an ACL. The **no** form of this command is used to cancel the configuration.

if-match ipv6 acl *acl-name*

no if-match ipv6 acl *acl-name*

Parameter Description

Parameter	Description
acl-name	ACL name

Defaults

No classification rule is configured in the system by default.

Command Mode

traffic classifier interface configuration mode

Usage Guide

You can use this command to specify an ACL as the classification rule of a traffic classifier. If data flows match the specified ACL, they meet the classification rule of the classifier.
The classification rule only applies to IPv6 packets.

Configuration Examples

Example 1: Configure all packets that match ACL 101 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match ipv6 acl ipv6acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

if-match ipv6 any

This command is used to set the classification rule of traffic classifier to matching any IPv6 packets. The **no** form of this command is used to cancel the configuration.

if-match ipv6 any

no if-match ipv6 any

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

Defaults By default, no classification matching rule is configured in the system.

Command Mode traffic classifier interface configuration mode

Usage Guide Use this command to match any IPv6 packets.
The classification rule only applies to IPv6 packets.

Configuration Examples Example 1: Any network packets are considered as matching the classification rule tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match ipv6 any
```

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

Platform Description N/A

if-match ipv6 dscp

This command is used to set the classification rule of a traffic classifier to matching DSCP value in IPv6 packets. The **no** form of this command is used to cancel the configuration.

if-match ipv6 dscp *dscp-value*

no if-match ipv6 dscp *dscp-value*

Parameter Description	**Parameter**	**Description**
	dscp-value	The DSCP value to be matched

Defaults No classification rule is configured in the system by default.

Command Mode traffic classifier interface configuration mode

Usage Guide You can use this command to specify the DSCP value in IPv6 packets as the classification rule of a traffic classifier. If data flows match the DSCP value, they meet the classification rule of the classifier.

The classification rule only applies to IPv6 packets.

Configuration Examples

Example 1: Configure packets whose DSCP value is 10 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match dscp 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

if-match mpls-exp

This command is used to set the classification rule of a traffic classifier to matching any MPLS packets. The **no** form of this command is used to cancel the configuration.

if-match mpls-exp *exp-value*

no if-match mpls-exp *exp-value*

Parameter Description

Parameter	Description
exp-value	The experimental value to be matched, ranging from 0 to 7

Defaults

No classification rule is configured in the system by default.

Command Mode

traffic classifier interface configuration mode

Usage Guide

You can use this command to specify the mpls experimental field value in packets as the classification rule of a traffic classifier. If data flows match the experimental value, they meet the classification rule of the classifier.
The classification rule only applies to MPLS packets.

Configuration Examples

Example 1: Configure packets whose experimental value is 1 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match mpls-exp 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

if-match source-mac

This command is used to set the classification rule of a traffic classifier to matching the source MAC address of Ethernet packets. The **no** form of this command is used to cancel the configuration.

if-match source-mac *mac-address*

no if-match source-mac *mac-address*

Parameter Description	**Parameter**	**Description**
	mac-address	Ethernet MAC address

Defaults No classification rule is configured in the system by default.

Command Mode traffic classifier interface configuration mode

Usage Guide You can use this command to specify the Ethernet source MAC address of packets as the classification rule of a traffic classifier. If data flows match the MAC address, they meet the classification rule of the classifier.
The classification rule only applies to Ethernet packets.

Configuration Examples Example 1: Configure packets that match the source MAC address 00d0.f822.33ac to match traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match source-mac 00d0.f822.33ac
```

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

Platform Description N/A

ip-dscp-inbound

This command is used to set the DSCP-based traffic policy for 802.1P inbound traffic in the diffserv domain. The **no** form of this command is used to restore the default policy.

ip-dscp-inbound *dscp-value* **phb** *service-class color*

no ip-dscp-inbound *dscp-value* **phb** *service-class color*

Parameter Description

Parameter	Description
dscp-value	The DSCP field value of IP packets, ranging from 0 to 63
service-class	Class of service mapped to a traffic class
color	Packet color corresponding to a traffic class

Defaults

By default, the IP inbound traffic policy exists in the diffserv domain.

Command Mode

diffserv domain configuration mode

Usage Guide

You can use this command to change the mapping between the DSCP value of IP packets and a CoS and discard priority. Combining the outbound traffic policy, you can enable a simple traffic policy. Hierarchical QoS (HQoS) supports eight classes of service, namely, cs7, cs6, ef, af1, af2, af3, af4, and be, which are described as follows:

Class of Service	Description
CS7	It is used for in-band control messages, with the highest priority.
CS6	It is used for protocol packets on the control plane, such as routing protocol packets and BFD packets.
EF (Expedited Forwarding)	It is used for services that require delay, jitter, and packet loss rate guarantees, such as VoIP and TDM.
AF4 Assured Forwarding AF3 AF2 AF1	Forwarding these services is assured when they do not exceed the maximum allowed bandwidth. Once they exceed the bandwidth, they will be discarded according to their priorities. These services fall into four categories, each allocated different bandwidth.
BE (Best Effort)	It is used for services not sensitive to delay, jitter, and packet loss, such as Internet services like Web and FTP.

HQoS supports green, yellow, and red, and supports configuration of different packet drop policies for these three colors using WRED.

Configuration Examples

Example 1: Map packets with the IP DSCP value of 32 to the CoS of EF and color green.

```
Ruijie(config)#diffserv domain ipdscp
Ruijie(config-diffserv-domain)#ip-dscp-inbound 32 phb ef green
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip-dscp-outbound

This command is used to set the traffic policy based on the CoS and discard priority for IP outbound traffic in the diffserv domain. The **no** form of this command is used to restore the default policy.

ip-dscp-outbound *service-class color* **map** *dscp-value*

no ip-dscp-outbound *service-class color* **map** *dscp-value*

Parameter Description

Parameter	Description
dscp-value	The DSCP field value of IP packets, ranging from 0 to 63
service-class	Class of service mapped to a traffic class
color	Packet color corresponding to a traffic class

Defaults

By default, the IP outbound traffic policy exists in the diffserv domain.

Command Mode

diffserv domain configuration mode

Usage Guide

You can use this command to change the mapping relationship between a CoS and a DSCP value for IP packets. Combining the inbound traffic policy, you can enable a simple traffic policy. Hierarchical QoS (HQoS) supports eight classes of service, namely, cs7, cs6, ef, af1, af2, af3, af4, and be, which are described as follows:

Class of Service		Description
CS7		It is used for in-band control messages, with the highest priority.
CS6		It is used for protocol packets on the control plane, such as routing protocol packets and BFD packets.
EF (Expedited Forwarding)		It is used for services that require delay, jitter, and packet loss rate guarantees, such as VoIP and TDM.
AF4	Assured Forwarding	Forwarding these services is assured when they do not exceed the maximum allowed bandwidth. Once they exceed the bandwidth, they will be discarded according to their priorities. These services fall into four categories, each allocated different bandwidth.
AF3		
AF2		
AF1		
BE (Best Effort)		It is used for services not sensitive to delay, jitter, and packet loss, such as Internet services like Web and FTP.

HQoS supports green, yellow, and red, and supports configuration of different packet drop policies for these three colors using WRED.

Configuration Examples

Example 1: Map packets with the CoS of EF and color green to the IP DSCP value of 32.

```
Ruijie(config)# diffserv domain ipdscp
Ruijie(config-diffserv-domain)#ip-dscp-outbound ef green map 32
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

port-bandwidth (interface)

This command is used to configure the bandwidth provided by the ISP for an AP member port. The **no** form of this command is used to remove the configuration.

port-bandwidth *bandwidth-value1*

no port-bandwidth

Parameter Description

Parameter	Description
bandwidth–value1	Max bandwidth provided by the ISP, ranging from 1 to 10000000 (Kbit/s)

Defaults No bandwidth is configured for an AP member port by default.

Command Mode Interface configuration mode

Usage Guide If the active port of the AP does not use the HQoS routing policy, this command does not take effect.

Configuration Examples

Example 1: Configure 2M bandwidth for AP member port Gi0/0.

```
Ruijie(config)#int gigabitethernet 0/1/1
Ruijie(config-if-Gigabitethernet 0/1/1)#port-queue pqt1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mpls-exp-inbound

This command is used to set the experimental value-based traffic policy for MPLS inbound traffic in the diffserv domain. The **no** form of this command is used to restore the default policy.

mpls-exp-inbound *exp-value* **phb** *service-class color*

no mpls-exp-inbound *exp-value* **phb** *service-class color*

Parameter Description

Parameter	Description
exp-value	The experimental field value of MPLS packets, ranging from 0 to 7
service-class	Class of service mapped to a traffic class
color	Packet color corresponding to a traffic class

Defaults By default, the MPLS inbound traffic policy exists in the diffserv domain.

Command Mode diffserv domain configuration mode

Usage Guide

You can use this command to change the mapping relationship between the experimental value of MPLS packets and a CoS and discard priority. Combining the outbound traffic policy, you can enable a simple traffic policy.

Hierarchical QoS (HQoS) supports eight classes of service, namely, cs7, cs6, ef, af1, af2, af3, af4, and be, which are described as follows:

Class of Service	Description
CS7	It is used for in-band control messages, with the highest priority.

CS6		It is used for protocol packets on the control plane, such as routing protocol packets and BFD packets.
EF (Expedited Forwarding)		It is used for services that require delay, jitter, and packet loss rate guarantees, such as VoIP and TDM.
AF4	Assured Forwarding	Forwarding these services is assured when they do not exceed the maximum allowed bandwidth. Once they exceed the bandwidth, they will be discarded according to their priorities. These services fall into four categories, each allocated different bandwidth.
AF3		
AF2		
AF1		
BE (Best Effort)		It is used for services not sensitive to delay, jitter, and packet loss, such as Internet services like Web and FTP.

HQoS supports green, yellow, and red, and supports configuration of different packet drop policies for these three colors using WRED.

Configuration Examples

Example 1: Map packets with the MPLS experimental value of 3 to the CoS of EF and color green.

```
Ruijie(config)#diffserv domain mplsexp
Ruijie(config-diffserv-domain)#mpls-exp-inbound 3 phb ef green
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

mpls-exp-outbound

This command is used to set the traffic policy based on the CoS and discard priority for MPLS outbound traffic in the diffserv domain. The **no** form of this command is used to restore the default policy.

mpls-exp-outbound *service-class color* **map** *exp-value*

no mpls-exp-outbound *service-class color* **map** *exp-value*

Parameter Description

Parameter	Description
exp-value	The experimental field value of MPLS packets, ranging from 0 to 7
service-class	Class of service mapped to a traffic class
color	Packet color corresponding to a traffic class

Defaults

By default, the MPLS outbound traffic policy exists in the diffserv domain.

Command Mode

diffserv domain configuration mode

Usage Guide

You can use this command to change the mapping relationship between a CoS and an experimental value for MPLS packets. Combining the inbound traffic policy, you can enable a simple traffic policy. Hierarchical QoS (HQoS) supports eight classes of service, namely, cs7, cs6, ef, af1, af2, af3, af4,

and be, which are described as follows:

Class of Service		Description
CS7		It is used for in-band control messages, with the highest priority.
CS6		It is used for protocol packets on the control plane, such as routing protocol packets and BFD packets.
EF (Expedited Forwarding)		It is used for services that require delay, jitter, and packet loss rate guarantees, such as VoIP and TDM.
AF4	Assured Forwarding	Forwarding these services is assured when they do not exceed the maximum allowed bandwidth. Once they exceed the bandwidth, they will be discarded according to their priorities. These services fall into four categories, each allocated different bandwidth.
AF3		
AF2		
AF1		
BE (Best Effort)		It is used for services not sensitive to delay, jitter, and packet loss, such as Internet services like Web and FTP.

HQoS supports green, yellow, and red, and supports configuration of different packet drop policies for these three colors using WRED.

Configuration Examples

Example 1: Map packets with the CoS of EF and color green to the MPLS experimental value of 3.

```
Ruijie(config)# diffserv domain mplsexp
Ruijie(config-diffserv-domain)#mpls-exp-outbound ef green map 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

port-queue

This command is used to enter the configuration layer of a port-queue template of a specific name. If the specified port-queue template does not exist, the system creates the template with the name. The **no** form of the command is used to delete the port-queue template of the name from the system.

port-queue *port-queue-name*

no port-queue *port-queue-name*

Parameter Description

Parameter	Description
port-queue-name	The name of the port-queue template

Command Mode

Global configuration mode

Usage Guide

You can use the port-queue command to create a port-queue template of the specific name and enter the port-queue interface configuration mode. You can configure scheduling parameters for eight port queues on the port-queue interface.

Configuration

Example 1: Configure scheduling parameters for different port queues in the port-queue template.

Examples

```
Ruijie(config)#port-queue pqt1
Ruijie(config-port-queue)# queue be lpq outbound
Ruijie(config-port-queue)# queue af1 wfq weight 10 shaping 100000 wred pwt1
Ruijie(config-port-queue)# queue cs7 pq shaping wred pwt1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

port-queue (interface)

This command is used to apply a port queue to an interface. The **no** form of this command is used to cancel the port queue on the interface.

port-queue *port-queue-name* [**shaping** *shaping-value]*

no port-queue *port-queue-name* [**shaping** *shaping-value]*

Parameter Description

Parameter	Description
shaping-value	Shaping value, ranging from 1 to 10000000 (Kbit/s)

Defaults No port queue is applied to any interface by default.

Command Mode Interface configuration mode

Usage Guide

The port queue must exist in the device; otherwise, you cannot apply the port queue to the interface. The traffic policy can only be applied to the outbound traffic of the interface.

Note that enabling the **port-queue** command on the interface will affect the QoS function as follows:

(1) If you configure GTS of QoS on the same interface, GTS rate limiting will not take effect.

(2) If you configure CQ, PQ, CBWFQ, WRED and RTPQ of QoS on the same interface, packets will not enter the corresponding queue and QoS queue scheduling will not take effect.

(3) If you remove this command configuration from an interface, QoS queue scheduling will be restored.

(4) If you configure this command on an interface, QoS CAR will not be affected.

Configuration Examples

Example 1: Apply port queue pqt1 to an interface.

```
Ruijie(config)#int gigabitethernet 0/1/1
Ruijie(config-if-Gigabitethernet 0/1/1)#port-queue pqt1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

port-res-queue

This command is used to mark the packet for resource reservation. The **no** form of this command is used to remove the configuration.

port-res-queue

no port-res-queue

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

Defaults No packet is marked for resource reservation by default.

Command Mode Traffic behavior interface configuration mode

Usage Guide

The packet associated with traffic behavior will be marked for resource reservation.

1. If the outbound interface is configured with a resource reservation queue, the packet enters the queue for scheduling.
2. If the outbound interface is not configured with a resource reservation queue, the packet enters the flow queue for scheduling based on its service-class.

Configuration Examples

Example 1: Mark the packet for resource reservation.

```
Ruijie(config)# traffic behavior tb1
Ruijie(config-port-queue)# port-res-queue
```

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

Platform Description N/A

port-res-queue (interface)

This command is used to apply the resource reservation queue to the interface. One queue is allowed for one interface and up to 16 queues for the device. The **no** form of this command is used to remove the configuration.

port-res-queue *shaping-value* [**depth** *depth-value*]

no port-res-queue

Parameter Description	**Parameter**	**Description**
	shaping-vlaue	Shaping value, ranging from 1 to 10000000 (Kbit/s).
	depth-value	Queue depth, ranging from 8 to 2048.

Defaults No queue is applied to any interface by default.

Command Mode	Interface configuration mode
Usage Guide	The resource reservation queue applied to the interface is scheduled for outbound traffic only. The resource reservation queue takes effect only after the **port-queue** command is run on the interface. The shaping value for the resource reservation queue is allocated form the shaping value configured in the **port-queue** command on the interface. The shaping value is automatically allocated only when there is a flow passing the resource reservation queue. When the flow stops for 3 minutes, the shaping value allocated to the resource reservation queue is invalidated.

Configuration Examples	Example 1: Apply the resource reservation queue to the interface.
	`Ruijie(config)#int gigabitethernet 0/1/1`
	`Ruijie(config-if-Gigabitethernet 0/1/1)# port-res-queue 5000 depth 300`

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

queue

This command is used to define scheduling parameters for eight queue priorities. The **no** form of this command is used the restore the default queue scheduling parameters.

queue *cos-value* {**pq** | **wfq weight** *weight-value* | **lpq**} [**shaping** *shaping-value*] [**wred** *wred-name*] [**depth** *depth-value*]

no queue *cos-value* {**pq** | **wfq weight** *weight-value* | **lpq**} [**shaping** *shaping-value*] [**wred** *wred-name*] [**depth** *depth-value*]

Parameter Description

Parameter	Description
cos-value	A flow-queue value
pq	The flow queue uses pq scheduling
wfq	The flow queue uses wfq scheduling
weight	Sets the weight for wfq
weight-value	The wfq weight value, ranging from 1 to 1024
lpq	The flow queue uses lpq scheduling
shaping	Flow queue shaping
shaping-value	The flow queue shaping rate, ranging from 1 to 10000000 (Kbit/s)
wred	The flow queue uses the user-defined WRED template for congestion avoidance
wred-name	The WRED template name
depth	Flow queue depth
depth-value	Flow queue depth, ranging from 8 to 2048, default value 200

Defaults

The system uses default flow-queue scheduling parameters by default:

CoS	Scheduling Policy	WFQ Weight	Shaping	wred
cs6	**PQ**	**-**	**None**	**None (tail discarded)**
cs7	**PQ**	**-**	**None**	**None (discarding the tail)**
e	**Q**	**-**	**None**	**None (tail discarded)**
af4	**WFQ**	**15**	**None**	**None (tail discarded)**
af3	**WFQ**	**15**	**None**	**None (tail discarded)**
af2	**WFQ**	**10**	**None**	**None (tail discarded)**
af1	**WFQ**	**10**	**None**	**None (tail discarded)**
e	**WFQ**	**10**	**None**	**None (tail discarded)**

Command Mode

flow-queue or port-queue interface configuration mode

Usage Guide

Each flow queue has its default scheduling parameters, which you can redefine using the queue command. Eight flow queues are supported, namely, ef, cs6, cs7, af1, af2, af3, af4, and be. Three scheduling methods are supported, namely, pq, wfq, and lpq.

The flow queue depth is adjusted according to the sudden burst in service demand. If the service demand increases significantly all of a sudden, the flow queue depth should be extended appropriately. When the a large number of queues are configured, you are suggested to decrease the queue depth to avoid impact on queue scheduling due to too excessive buffered packets for some queues.

Configuration Examples

Example 1: Configure scheduling parameters for different flow-queue priorities in the flow-queue template.

```
Ruijie(config)#flow-queue fqt1
Ruijie(config-flow-queue)# queue be lpq
Ruijie(config-flow-queue)# queue af1 wfq weight 10 shaping 100000 wred wt1
Ruijie(config-flow-queue)# queue cs7 pq shaping wred wt1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

remark

This command is used to set the precedence or experimental value for packets. The **no** form of this command is used to cancel the precedence or experimental value setting.

remark [**dscp** *dscp-value* | **ip-precedence** *ip-precedence-value* | **mpls-exp** *mpls-exp-value* | **ipv6 dscp** *ipv6-dscp-value* | **cos** *cos-value*]

no remark [**dscp** *dscp-value* | **ip-precedence** *ip-precedence-value* | **mpls-exp** *mpls-exp-value*]

Parameter Description

Parameter	Description
dscp	Resets the DSCP field value for IPv4 packets
dscp-value	The DSCP value to be set
ip-precedence	Resets the precedence field value for IPv4 packets
ip-precedence-value	The precedence field value to be set
mpls-exp	Resets the experimental value for MPLS packets
mpls-exp-value	The experimental value to be set
ipv6 dscp	Resets the DSCP field value for IPv6 packets
ipv6-dscp-value	The DSCP value to be set
cos	Resets the CoS value for Ethernet 802.1P packets
cos-value	The CoS value to be set

Defaults The traffic behavior rules do not reset the precedence or experimental value for packets by default.

Command Mode traffic behavior configuration mode

Usage Guide

The remark command can be used to change the precedence and DSCP values to be applicable only to IPv4 packets.
The remark command can be used to change the mpls-exp value to be applicable only to MPLS packets.
The remark command can be used to change the IPv6 DSCP value to be applicable only to IPv6 packets.
The remark command can be used to change the 802.1P CoS value to be applicable only to 802.1P packets.
Complex traffic CoS marking only supports policies with the traffic class and traffic behavior of the same network. For example, when the MPLS flow features are matched, the MPLS precedence is marked.

Configuration Examples

Example 1: Define a traffic behavior rule, which uses the user queue template uq1 and marks the packets with a CoS of EF green color. Reset the DSCP value to 40 for packets using this rule.

```
Ruijie(config)#traffic behavior tb1
Ruijie(config-traffic-behavior)#user-queue uq1 inbound
Ruijie(config-traffic-behavior)#service-class ef color green
Ruijie(config-traffic-behavior)#remark dscp 40
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

service-class

This command is used to color packets of different CoSs. The **no** form of this command is used to restore the default coloring mechanism.

service-class *service-class-value* **color {green | yellow | red}**

no service-class *service-class -value* **color {green | yellow | red**}

Parameter Description

Parameter	Description
service-class-value	Eight CoSs supported: ef, cs6, cs7, af1, af2, af3, af4, and be
color	Colors packets
green | *yellow* | *red*	Three colors of packets

Defaults No color rule is associated by default.

Command Mode traffic behavior interface configuration mode

Usage Guide

Each traffic behavior rule uses a default mapping relationship to prioritize and color packets. You can use the service-class command to configure colors for packets of different CoSs.
Hierarchical QoS (HQoS) supports eight classes of service, namely, cs7, cs6, ef, af1, af2, af3, af4, and be, which are described as follows:

Class of Service		Description
CS7		It is used for in-band control messages, with the highest priority.
CS6		It is used for protocol packets on the control plane, such as routing protocol packets and BFD packets.
EF (Expedited Forwarding)		It is used for services that require delay, jitter, and packet loss rate guarantees, such as VoIP and TDM.
AF4	Assured Forwarding	Forwarding these services is assured when they do not exceed the maximum allowed bandwidth. Once they exceed the bandwidth, they will be discarded according to their priorities. These services fall into four categories, each allocated different bandwidth.
AF3		
AF2		
AF1		
BE (Best Effort)		It is used for services not sensitive to delay, jitter, and packet loss, such as Internet services like Web and FTP.

HQoS supports green, yellow, and red, and supports configuration of different packet drop policies for these three colors using WRED.
If the traffic behavior does not have a color rule, packets of the CoS of BE are colored green.

Configuration Examples

Example 1: Define a traffic behavior rule, which uses the user queue template uq1 and colors the packets of the CoS of EF green . Reset the DSCP value to 40 for packets using this rule.

```
Ruijie(config)#traffic behavior tb1
```

```
Ruijie(config-traffic-behavior)#user-queue uq1 inbound
Ruijie(config-traffic-behavior)#service-class ef color green
Ruijie(config-traffic-behavior)#remark dscp 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

shaping

This command is used to set the traffic shaping rate for user queues. The **no** form of this command is used to disable traffic shaping for user queues.

shaping *shaping-value*

no shaping *shaping-value*

Parameter Description

Parameter	Description
shaping-value	The upper limit of the traffic shaping rate for user queues, ranging from 1 to 10000000 (Kbit/s)

Defaults Traffic shaping is disabled for user queues by default.

Command Mode user-group-queue configuration mode

Usage Guide User group queue traffic shaping is applicable to all traffic of that user group. A cache and token bucket are used to complete shaping. The packets that are forwarded too fast are first buffered in the cache, and then they are forwarded evenly under control of the token bucket.

Configuration Examples Example 1: Configure user group queue traffic shaping.

```
Ruijie(config)#user-group-queue ugq1 inbound
Ruijie(config-user-group-queue)#shaping 100000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

sub-traffic-policy

This command is used to specify a sub-traffic policy in a traffic behavior, and the sub-traffic policy should be created in advance. The **no** form of this command is used to delete the sub-traffic policy.

sub-traffic-policy *traffic-policy-name*

no sub-traffic-policy *traffic-policy-name*

Parameter Description	Parameter	Description
	traffic-policy-name	The name of the traffic policy

Defaults No sub-traffic policy is associated with the traffic behavior by default.

Command Mode Traffic behavior configuration mode

Usage Guide The sub-traffic-policy command allows you to specify a sub-traffic policy in the traffic behavior to create embedded policies.
The system does not allow multiple sub-policies to form a loop by one sub-policy containing another nested sub-policy.

Configuration Examples **Example 1: Configure sub-traffic policy subtp1 in traffic behavior tb1. In this way, the sub-traffic policy is applied to the data that match the classification rules of tb1.**

```
Ruijie(config)#traffic behavior tb1
Ruijie(config-traffic-behavior)#sub-traffic-policy subtp1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

traffic behavior

This command is used to enter the configuration layer of the traffic behavior of a specific name. If the specified traffic behavior does not exist, the system creates the traffic behavior with the name. The **no** form of the command is used to delete the traffic behavior of the name from the system.

traffic behavior *behavior-name*

no traffic behavior *behavior-name*

Parameter Description	Parameter	Description
	behavior-name	The name of a traffic behavior

Defaults No traffic behavior is configured in the system by default.

Command Mode Global configuration mode

Usage Guide You can use the traffic behavior command to create a traffic behavior of the specific name and enter the traffic behavior interface configuration mode. You can configure the user queue template, packet color rules, and remark activities on the traffic behavior interface.

Configuration Examples

Example 1: Define a traffic behavior rule, which uses the user queue template uq1 and colors the packets with a CoS of EF green. Reset the DSCP value to 40 for packets using this rule.

```
Ruijie(config)#traffic behavior tb1
Ruijie(config-traffic-behavior)#user-queue uq1 inbound
Ruijie(config-traffic-behavior)#service-class ef color green
Ruijie(config-traffic-behavior)#remark dscp 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

traffic classifier

This command is used to enter the configuration layer of a traffic classifier of a specific name. If the traffic classifier of the name does not exist, the system creates the traffic classifier with the name. The **no** form of the command is used to delete the traffic classifier of the name from the system.

traffic classifier *classifier-name* [**and** | **or**]

no traffic classifier *classifier-name*

Parameter Description

Parameter	Description
classifier-name	Traffic classifier name, which is also the ID to distinguish the classifier in the system
**and	or**	Type of the traffic classifier, indicating whether all or one of the conditions in the classifier should be matched

Defaults

No traffic classifier is configured in the system by default. The type of a new traffic classifier is “or”, which means only one condition in the classifier needs to be matched.

Command Mode

Global configuration mode

Usage Guide

You can use the traffic classifier command to create a traffic classifier of the specific name and enter the traffic-classifier interface configuration mode. You can configure the data classification rules based on your needs on the traffic-classifier interface. The following 11 classification rules are supported:

1. if-match acl
2. if-match dscp
3. if-match ip-precedence
4. if-match cos
5. if-match mpls-exp
6. if-match any
7. if-match ipv6 dscp
8. if-match ipv6 acl

9. if-match ipv6 any

10. if-match destination-mac

11. if-match source-mac

Configuration Examples

Example 1: Configure all packets that match ACL 101 to meet the classification rule of traffic classifier tcr1.

```
Ruijie(config)#traffic classifier tcr1
Ruijie(config-traffic-classifier)#if-match acl 101
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

traffic policy

This command is used to enter the configuration layer of a traffic policy of a specific name. If the traffic policy of the name does not exist, the system creates the traffic policy with the name. The **no** form of the command is used to delete the traffic policy of the name from the system.

traffic policy *policy-name*

no traffic policy *policy-name*

Parameter Description

Parameter	Description
policy-name	Traffic policy name

Defaults

No traffic policy is configured in the system by default.

Command Mode

Global configuration mode

Usage Guide

You can use the traffic policy command to create a traffic policy of the specific name and enter the traffic-policy interface configuration mode. You can associate a traffic classifier rule with a traffic behavior rule on the traffic-policy interface.

Multiple traffic classifiers and traffic behaviors can be associated in a traffic policy, and precedence values are given to differentiate traffic policies, a smaller value representing a higher priority. The first-match-quit mode is adopted for the traffic classifiers and traffic behaviors in a traffic policy, which means that once the first traffic classifier/behavior is matched, the traffic policy is quitted.

Configuration Examples

Example 1: The traffic classifier rule tcr1 is associated with traffic behavior rule tbr1 in traffic policy tp1. In this way, actions in tbr1 are implemented for the network traffic that matches tcr1.

```
Ruijie(config)#traffic policy tp1
Ruijie(config-traffic-policy)#classifier tcr1 behavior tbr1 precedence 1
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

traffic-policy

This command is used to apply a traffic policy to an interface. The **no** form of this command is used to cancel application of the traffic policy on the interface.

traffic-policy *policy-name* [**inbound | outbound] [linklayer | all-layer**]

no traffic-policy *policy-name* [**inbound | outbound] [linklayer | all-layer**]

Parameter Description

Parameter	Description
policy-name	Traffic policy name

Defaults The system does not configure any traffic policy to an interface by default.

Command Mode Interface configuration mode

Usage Guide

The traffic policy must exist in the device; otherwise, you cannot apply the traffic policy to the interface.

By default, the traffic policy applies to IPv4 and IPv6 L3 packets and MPLS packets if the layer parameter is not specified; it applies to 802.1P L2 packets only if the linklayer parameter is specified; it applies to L3 and L2 packets if the all-layer parameter is configured.

When the linklayer and all-layer parameters are specified, the traffic policy can only be configured for the main interface, and it applies to the main interface and all associated subinterfaces after configuration. This command cannot be configured for a subinterface when these two parameters are specified.

The linklayer and all-layer parameters are not configured on the ATM main interface and subinterfaces.

Configuration Examples

Example 1: Apply traffic policy tp1 to the inbound traffic on the interface.

```
Ruijie(config)#int gigabitethernet 0/1
Ruijie(config-if-Gigabitethernet 0/1)#traffic-policy tp1 inbound
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

trust 8021p

This command is used to enable 8021p associated with an interface in a diffserv domain. The **no** form of this command is used to disable the 8021p policy.

trust 8021p

no trust 8021p

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the 8021p associated with an interface in a diffserv domain is disabled.

Command Mode Interface configuration mode

Usage Guide You can use this command to enable the 8021p policy associated with an interface in a diffserv domain. The 8021p policy in a diffserv domain is disabled by default.
This command can only be configured for a main interface, and it applies to all subinterfaces associated with the main interface after configuration. It cannot be configured for a subinterface.
This command cannot be configured on ATM main interface and subinterfaces.

Configuration Examples Example 1: Enable 8021p associated with the interface in a diffserv domain.

```
Ruijie(config)#interface gigabitethernet 0/1/1.1
Ruijie(config-if-Gigabitethernet 0/1/1.1)#trust upstream 8021p
Ruijie(config-if-Gigabitethernet 0/1/1.1)#trust 8021p
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

trust upstream

This command is used to associate a diffserv domain with an interface and apply its traffic policy. The **no** form of this command is used to cancel the diffserv domain associated and traffic policy.

trust upstream {*ds-domain-name* | **default**}

no trust upstream {*ds-domain-name* | **default**}

Parameter Description	Parameter	Description
	ds-domain-name	The name of the diffserv domain

Defaults No diffserv domain is associated with the interface by default.

Command Mode Interface configuration mode

Usage Guide You can associate a diffserv domain with the interface, so as to use the upstream traffic policy to establish mapping between the diffserv domain precedence and a CoS and discard priority for

upstream traffic on the interface, and to use the downstream traffic policy to establish mapping between a CoS and discard priority and the diffserv domain precedence for downstream traffic on the interface.
Mapping between 802.1p and the diffserv domain precedence is not supported by default. You need to use the trust 8021p command to make the mapping effective.

Configuration Examples

Example 1: Associate the interface with diffserv domain mplsexp.

```
Ruijie(config)#interface gigabitethernet 1/1/1
Ruijie(config-if-Gigabitethernet 1/1/1)#trust upstream mplsexp
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

user-group-queue

This command is used to enter the configuration layer of a user group queue of a specific name. If the specified user group queue does not exist, the system creates the user group queue with the name. The **no** form of the command is used to delete the user group queue of the name from the system.

user-group-queue *user-group-queue-name* [**inbound | outbound**]

no user-group-queue *user-group-queue-name* [**inbound | outbound**]

Parameter Description

Parameter	Description
user-group-queue-name	The name of a user group queue
inbound | *outbound*	Direction of a user group queue, inbound or outbound

Defaults

No user group is configured in the system by default.

Command Mode

Global configuration mode

Usage Guide

You can use the user-group-queue command to create a user group of the specific name and enter the user-group-queue interface configuration mode. You can set the upper limit of traffic shaping for the user group on the user-group-queue interface.

Note

If user groups are on different service cards of a distributed device, the user group queue is working on its service card separately.

Configuration Examples

Example 1: Set the upper limit of traffic shaping for user group ugq1.

```
Ruijie(config)#user-group-queue ugq1 inbound
Ruijie(config-user-group-queue)#shaping 100000
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

user-group-queue (user-queue)

The **user-group-queue** command is used under a user-queue to associate the user queue with the specified user group queue template, so that the user queue is scheduled according to template parameters. The no form of this command is used the restore the default flow-queue parameters.

user-group-queue *user-group-queue-name*

no user-group-queue *user-group-queue-name*

Parameter Description	Parameter	Description
	user-group-queue-name	The name of a user group queue

Defaults A user queue does not belong to any user group by default.

Command Mode use-queue interface configuration mode

Usage Guide The user group queue template must exist in the device; otherwise, you cannot associate the user group template with the user queue.

Configuration Examples Example 1: Associate user group queue ugq1 with user group uq1.

```
Ruijie(config)#user-queue uq1 inbound
Ruijie(config-user-queue)#user-group-queue ugq1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

user-queue

This command is used to enter the configuration layer of a user queue of a specific name. If the specified user queue does not exist, the system creates the user queue with the name. The **no** form of the command is used to delete the user queue of the name from the system.

user-queue *user-queue-name* [**inbound | outbound**]

no user-queue *user-queue-name* [**inbound | outbound**]

Parameter	Parameter	Description

Description

user-queue-name	The name of a user queue
inbound | outbound	Direction of a user queue, inbound or outbound

Defaults No user queue is configured in the system by default.

Command Mode Global configuration mode

Usage Guide

You can use the user-queue command to create a user queue of the specific name and enter the user-queue interface configuration mode. You can configure scheduling parameters for the user queue based on your needs on the user-queue interface.


Note If users are on different service cards of a distributed device, the user queue is working on its service card separately.

Configuration Examples

Example 1: Configure a user queue.

```
Ruijie(config)#user-queue uq1 inbound
Ruijie(confg-user-queue)#cir 100000 pir 100000
Ruijie(config-user-queue)#flow-queue fqt1
Ruijie(config-user-queue)#user-group-queue ugq1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

user-queue (traffic behavior)

The **user-queue** command is used under the traffic behavior configuration mode to configure user queue scheduling parameters in the traffic behavior rule. The **no** form of this command is used the restore the default user queue scheduling parameters.

user-queue *user-queue-name* **[inbound | outbound]**

no user-queue *user-queue-name* **[inbound | outbound]**

Parameter Description

Parameter	Description
user-queue-name	The name of a user queue
inbound | outbound	Direction of a user queue, inbound or outbound

Defaults No user queue rule s associated by default.

Command Mode traffic behavior interface configuration mode

Usage Guide

The user queue template must exist in the device; otherwise, you cannot apply the template to the traffic behavior.
If no user queue rule is associated with the traffic behavior, the CoS of BE is used for scheduling by default.

Configuration Examples

Example 1: Define a traffic behavior rule, which uses the user queue template uq1 and colors the packets with a CoS of EF green . Reset the DSCP value to 40 for packets using this rule.

```
Ruijie(config)#traffic behavior tb1
Ruijie(config-traffic-behavior)#user-queue uq1 inbound
Ruijie(config-traffic-behavior)#service-class ef color green
Ruijie(config-traffic-behavior)#remark dscp 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

wred

This command is used to enter the configuration layer of WRED template of a specific name. If the WRED template of the name does not exist, the system creates a WRED template with the name. The **no** form of the command is used to delete the WRED template of the name from the system.

wred *wred-name*

no wred *wred-name*

Parameter Description

Parameter	Description
wred-template-name	The WRED template name

Defaults

No WRED template is configured in the system by default.

Command Mode

Global configuration mode

Usage Guide

You can use the wred command to create the specified WRED template and enter the WRED interface configuration mode. You can set the discard thresholds and discard percentages for three colors of packets on the WRED interface.

Configuration Examples

Example 1: The WRED template wt1 defines the discard thresholds and discard percentages for three colors of packets.

```
Ruijie(config)#wred wt1
Ruijie(config-wred)#color green low-limit 40 high-limit 60 discard-percent 10
Ruijie(config-wred)#color yellow low-limit 30 high-limit 50 discard-percent
10
```

```
Ruijie(config-wred)#color red low-limit 20 high-limit 40 discard-percent 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show diffserv domain

This command is used to show the configuration of a diffserv domain.

show diffserv domain *diffserv-domain-name [8021p-inbound* | *8021p-outbound* | *ip-dscp-inbound* | *ip-dscp-outbound* |*mpls-exp-inbound* | *mpls-exp-outbound]*

Parameter Description

Parameter	Description
diffserv-domain-name	The name of the diffserv domain
8021p-inbound	Mapping between the 802.1P priority and a CoS and discard priority
8021p-outbound	Mapping between a CoS and discard priority and the 802.1P priority
ip-dscp-inbound	Mapping between the ip-dscp priority and a CoS and discard priority
ip-dscp-outbound	Mapping between a CoS and discard priority and the ip-dscp priority
mpls-exp-inbound	Mapping between the mpls-exp priority and a CoS and discard priority
mpls-exp-outbound	Mapping between a CoS and discard priority and the mpls-exp priority.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the configuration of a diffserv domain in the system.

Configuration Examples

Example 1: Show the configuration of diffserv domain "ipdscp".

```
Ruijie# show diffserv domain ipdscp
IP-DSCP map to Server-class and Color :
  0 --> be    green
  1 --> be    green
  2 --> be    green
  3 --> be    green
  4 --> be    green
  5 --> be    green
  6 --> be    green
  7 --> be    green
  8 --> af1   green
  9 --> be    green
 10 --> af1   green
```

```
11 --> be   green
12 --> af1  yellow
13 --> be   green
14 --> af1  red
15 --> be   green
16 --> af2  green
17 --> be   green
18 --> af2  green
19 --> be   green
20 --> af2  yellow
21 --> be   green
22 --> af2  red
23 --> be   green
24 --> af3  green
25 --> be   green
26 --> af3  green
27 --> be   green
28 --> af3  yellow
29 --> be   green
30 --> af3  red
31 --> be   green
32 --> af4  green
33 --> be   green
34 --> af4  green
35 --> be   green
36 --> af4  yellow
37 --> be   green
38 --> af4  red
39 --> be   green
40 --> ef   green
41 --> be   green
42 --> be   green
43 --> be   green
44 --> be   green
45 --> be   green
46 --> ef   green
47 --> be   green
48 --> cs6  green
49 --> be   green
50 --> be   green
51 --> be   green
52 --> be   green
53 --> be   green
54 --> be   green
55 --> be   green
```

```
56 --> cs7   green
57 --> be    green
58 --> be    green
59 --> be    green
60 --> be    green
61 --> be    green
62 --> be    green
63 --> be    green
```

```
MPLS-EXP map to Server-class and Color :
 0 --> be    green
 1 --> af1   green
 2 --> af2   green
 3 --> af3   green
 4 --> af4   green
 5 --> ef    green
 6 --> cs6   green
 7 --> cs7   green
```

```
VLAN-Cos map to Server-class and Color :
 0 --> be    green
 1 --> af1   green
 2 --> af2   green
 3 --> af3   green
 4 --> af4   green
 5 --> ef    green
 6 --> cs6   green
 7 --> cs7   green
```

```
Server-class and Color map to IP-DSCP :
be    green    -->  0
be    yellow   -->  0
be    red      -->  0
af1   green    --> 10
af1   yellow   --> 12
af1   red      --> 14
af2   green    --> 18
af2   yellow   --> 20
af2   red      --> 22
af3   green    --> 26
af3   yellow   --> 28
af3   red      --> 30
af4   green    --> 34
af4   yellow   --> 36
af4   red      --> 38
```

```
ef   green   --> 46
ef   yellow  --> 46
ef   red     --> 46
cs6  green   --> 48
cs6  yellow  --> 48
cs6  red     --> 48
cs7  green   --> 56
cs7  yellow  --> 56
cs7  red     --> 56
```

```
Server-class and Color map to MPLS-EXP :
be   green   -->  0
be   yellow  -->  0
be   red     -->  0
af1  green   -->  1
af1  yellow  -->  1
af1  red     -->  1
af2  green   -->  2
af2  yellow  -->  2
af2  red     -->  2
af3  green   -->  3
af3  yellow  -->  3
af3  red     -->  3
af4  green   -->  4
af4  yellow  -->  4
af4  red     -->  4
ef   green   -->  5
ef   yellow  -->  5
ef   red     -->  5
cs6  green   -->  6
cs6  yellow  -->  6
cs6  red     -->  6
cs7  green   -->  7
cs7  yellow  -->  7
cs7  red     -->  7
```

```
Server-class and Color map to VLAN-CoS :
be   green   -->  0
be   yellow  -->  0
be   red     -->  0
af1  green   -->  1
af1  yellow  -->  1
af1  red     -->  1
af2  green   -->  2
af2  yellow  -->  2
```

```
af2   red     -->  2
af3   green    -->  3
af3   yellow   -->  3
af3   red     -->  3
af4   green    -->  4
af4   yellow   -->  4
af4   red     -->  4
ef    green    -->  5
ef    yellow   -->  5
ef    red     -->  5
cs6   green    -->  6
cs6   yellow   -->  6
cs6   red     -->  6
cs7   green    -->  7
cs7   yellow   -->  7
cs7   red     -->  7
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show flow-queue

The **show flow-queue** command is used to show the configuration of a flow queue.

show flow-queue [*flow-queue-name*]

Parameter Description	Parameter	Description
	flow-queue-name	The name of the flow queue

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the configuration of a flow queue in the system. If no flow queue name is specified, the configuration of all flow queues is shown by default.

Configuration Examples Example 1: Show the configuration of flow queue fq1.

```
Ruijie# show flow-queue fq1
flow queue fq1:
queue be wfq weight 10
queue af1 wfq weight 10
queue af2 wfq weight 10
queue af3 wfq weight 15
```

```
queue af4 wfq weight 15
queue ef pq
queue cs6 pq
queue cs7 pq
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

Command History	Version	Description
	10.4 (3b5)	Newly-added command

show port-queue

This command is used to show the port-queue configuration in the system.

show port-queue [*port-queue-name*]

Parameter Description	Parameter	Description
	port-queue-name	The name of the port-queue

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the port-queue configuration in the system. If no port-queue name is specified, the configuration of all port-queues is shown by default.

Configuration Examples Example 1: Show the configuration of a port-queue on the system interface.

```
Ruijie# show port-queue pqt1
port queue pqt1:
queue be wfq weight 10
queue af1 wfq weight 10
queue af2 wfq weight 10
queue af3 wfq weight 15
queue af4 wfq weight 15
queue ef pq
queue cs6 pq
queue cs7 pq
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show port-queue statistics

Parameter Description

This command is used to show the port-queue statistics of an interface in the system.

show port-queue statistics [interface *interface*]

Parameter	Description
Interface	The interface where port-queue is configured

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the port-queue statistics in the system. If no interface is specified, the statistics of all port-queues are shown by default.

Configuration Examples

Example 1: Show the port-queue statistics of interface gigabitethernet 1/1/1.

```
Ruijie# show port-queue interface gigabitethernet 1/1/1
[be]
  Pass:     42900556 packets,   2745666258 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,      2073046 balance,
0 token
[af1]
  Pass:     43401132 packets,   2608782540 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,         8960 balance,
0 token
[af2]
  Pass:     45091586 packets,   2707371120 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,      2069592 balance,
0 token
[af3]
  Pass:     43496828 packets,   2613966540 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,      2092532 balance,
0 token
[af4]
  Pass:     45170464 packets,   2711553720 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,      2092532 balance,
0 token
```

```
[ef]
  Pass:     45099831 packets,   2708775960 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,           0 balance,
0 token
[cs6]
  Pass:     46002386 packets,   2761254360 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,           0 balance,
0 token
[cs7]
  Pass:     41955096 packets,   2520579480 bytes
  Drop:           0 packets,           0 bytes
  Que :           0 packets,           0 bytes,           0 balance,
0 token
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show traffic classifier

This command is used to show the configuration of a traffic classifier in the system.

show traffic classifier [*classifier-name*]

Parameter Description	Parameter	Description
	classifier-name	The name of a traffic classifier

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the configuration of a traffic classifier in the system. If no traffic classifier name is specified, the configuration of all traffic classifiers is shown by default.

Configuration Examples Example 1: Show the configuration of traffic classifier tc1.

```
Ruijie# show traffic classifier tc1
traffic classifier tc1 or
  if-match acl 1501
```

Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

show traffic behavior

This command is used to show the configuration of a traffic behavior in the system.

show traffic behavior [*behavior-name*]

Parameter Description	**Parameter**	**Description**
	behavior-name	The name of a traffic behavior

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	You can use this command to show the configuration of a traffic behavior in the system. If no traffic behavior name is specified, the configuration of all traffic behaviors is shown by default.

Configuration Examples

Example 1: Show the configuration of traffic behavior tb1.

```
Ruijie# show traffic behavior tb1
traffic behavior tbu1
  user-queue uq1 inbound
  sub-traffic-policy sub
```

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

Platform Description	N/A

show traffic policy

This command is used to show the configuration of a traffic policy in the system.

show traffic policy [*policy-name*]

Parameter Description	**Parameter**	**Description**
	policy-name	Traffic policy name

Defaults	N/A
Command Mode	Privileged user mode
Usage Guide	You can use this command to show the configuration of a traffic policy in the system. If no traffic policy name is specified, the configuration of all traffic policies is shown by default.

Configuration Examples

Example 1: Show the configuration of traffic policy tp1.

```
Ruijie# show traffic policy tp1
traffic policy sub
  classifier 101 behavior 101 precedence 1
  classifier 102 behavior 102 precedence 2
  classifier 103 behavior 103 precedence 3
  classifier 104 behavior 104 precedence 4
  classifier 105 behavior 105 precedence 5
  classifier 106 behavior 106 precedence 6
  classifier 107 behavior 107 precedence 7
  classifier 108 behavior 108 precedence 8
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show user-group-queue

This command is used to show the statistics of all user group queues in the system.

show user-group-queue

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the statistics of all user group queues in the system.

Configuration Examples

Example 1: Show the statistics of all user group queues.

```
Ruijie# show user-group-queue

user-group-queue ugq1 inbound
 shaping 30000

user-group-queue ugq1 outbound
 shaping 4000
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

show user-group-queue statistics

This command is used to show the statistics of a user group queue in the system.

show user-group-queue statistics *user-group-queue-name* {**inbound | outbound}**

Parameter Description	**Parameter**	**Description**
	user-group-queue-name	The name of a user group queue

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	You can use this command to show the statistics of a user group queue in the system. If no device ID is specified, the statistics of a user group queue in the local device is shown by default. The device ID can be calculated using the slot and subslot: devid=slot*3+subslot. You can use the show version slot command to check the slot and subslot information in the slot field.

Configuration Examples

Example 1: Show the statistics of user group queue ugq1 in the local device.

```
Ruijie# show user-group-queue statistics ugq1 inbound
Pass:     27505335 packets,    2488832586 bytes
Drop:           0 packets,           0 bytes
Que :      1280000 token
```

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

Platform Description	N/A

show user-queue

This command is used to show the statistics of all user queues.

show user-queue

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

Defaults	N/A
Command Mode	Privileged user mode

Usage Guide You can use this command to show the statistics of all user queues.

Configuration Examples

Example 1: Show the statistics of all user queues.

```
Ruijie# show user-queue

user-queue uq1 inbound
 cir 100 pir 100
 flow-queue fq1
 user-group-queue ugq1
 flow-mapping fm1

user-queue uq2 inbound
 cir 300 pir 300

user-queue uq1 outbound
 cir 200 pir 200
 user-group-queue ugq1
 flow-mapping fm1

user-queue uq2 outbound
 cir 400 pir 400
 flow-queue fq2
 user-group-queue ugq1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show user-queue statistics

This command is used to show the statistics of a user queue.

show user-queue statistics *user-group-queue-name* {**inbound | outbound**}

Parameter Description

Parameter	Description
user-queue-name	The name of a user queue

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the statistics of a user queue in the system. If no device ID is specified, the statistics of a user queue in the local device is shown by default.
The device ID can be calculated using the slot and subslot: devid=slot*3+subslot. You can use the

show version slot command to check the slot and subslot information in the slot field.

Configuration Examples

Example 1: Show the statistics of user queue uq1 in the local device.

```
Ruijie# show user-queue statistics uq1 inbound
[be]
  Pass:       417629 packets,     39257126 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,      2069822 balance,
0 token
[af1]
  Pass:       452378 packets,     40714020 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,        39740 balance,
0 token
[af2]
  Pass:       445824 packets,     40124250 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,        87330 balance,
0 token
[af3]
  Pass:       439811 packets,     39583080 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,      2087162 balance,
0 token
[af4]
  Pass:       434429 packets,     39098610 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,      2087432 balance,
0 token
[ef]
  Pass:       429747 packets,     38677230 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,            0 balance,
0 token
[cs6]
  Pass:       423563 packets,     38120670 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,            0 balance,
0 token
[cs7]
  Pass:       399735 packets,     35976150 bytes
  Drop:            0 packets,           0 bytes
  Que :            0 packets,           0 bytes,            0 balance,
0 token
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show wred

This command is used to show the WRED configuration in the system.

show wred [*wred-name*]

Parameter Description	Parameter	Description
	wred-name	WRED name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to show the information of a WRED template in the system. If no WRED name is specified, the configuration of all WRED templates is shown by default.

Configuration Examples Example 1: Show the configuration of WRED template wt1.

```
Ruijie# show wred wt1
wred template wt1:
 color   low-limit  high-limit  discard-pecent
 green   70         100         100
 yellow  60         90          100
 red     50         80          100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

MPLS QOS Commands

default

This command specifies the action of table-map when the required mapping relation doesn't exist in the table-map. Use **no** form of this command to restore the action of table-map to default setting.

default { *default-value* **| copy | ignore** }

no default { *default-value* **| copy | ignore** }

Parameter description

Parameter	Description
default-value	Default mapping in the table-map (range: 0-99)

Default

The default action of table-map is "copy".

Command mode

Table-map interface configuration mode.

Usage guidelines

1. Configure default-value, which will be mapped when the mapping relation required doesn't exist.
2. Configure **copy**, which will copy the value to be mapped when the mapping relation required doesn't exist.
3. Configure **ignore**, which will ignore this mapping request when the mapping relation required doesn't exist.

Examples

Example 1: The following example configures the default-value of table-map named "tablemap1" as 8.

```
defalut 8
```

Example 2: The following example configures the action of table-map named "tablemap1" as copy.

```
defalut copy
```

Example 3: The following example configures the action of table-map named "tablemap1" as ignore.

```
defalut ignore
```

Related commands

Command	Description
N/A	N/A

Platform description

NA

map

This command adds a mapping entry to the table-map. Use **no** form of this command to delete the corresponding mapping relation from the system.

map from *from-value* **to** *to-value*

no map from *from-value* **to** *to-value*

Parameter description

Parameter	Description
from-value	The "map from" value, which will be mapped to the "to-value".
to-value	The "map to" value (range: 0-99), to which a value will be mapped if this value equals to "from-value".

Default

By default, no mapping policy is configured by the system.

Command mode

Table-map interface configuration mode.

Usage guidelines

By default, from-value and to-value must fall within the range of 0-99.

When an application (such as QoS) uses this table-map, the application (such as QoS) can specify the range of from-value and to-value in the table-map (for example, MPLS QoS requires that from-value and to-value must fall within the range of [0-7]).

If the data in table-map cannot meet the requirement of such application (such as QoS), table-map won't be used.

If the data in table-map meet the requirement imposed by the application (such as QoS), then the range of from-value and to-value in table-map will be changed to the range required by such application (for example: if MPLS QoS requires that from-value and to-value must fall within the range of [0-7] and if the data in the table-map meet its requirement, then the range of from-value and to-value in table-map will become [0-7], and mappings added later must fall within this range).

Examples

Example 1: The following example adds a mapping (34 to 56) into the table-map named tablemap1.

```
map from 34 to 56
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

match mpls

This command configures the class-map to use mpls encapsulation protocol type as the match rule. Use **no** form of this command to disable the configuration.

match mpls experimental { *exp-value, exp-value…* }

no match mpls experimental { *exp-value, exp-value…* }

Parameter description

Parameter	Description
exp-value	The experimental value to be matched (range: 0-7).

Default By default, no match rule is configured by the system.

Command mode Class-map interface configuration mode

Usage guidelines The user can configure this command to use the value of mpls experimental field in data packets as the match rule of class-map. If the value is matched, the packets will be put into the corresponding CBWFQ queue. The user can configure multiple values in this command, and if values are repeated or aren't organized from small to large, the system will automatically adjust the command to merge or organize the values.

Examples Example 1: In the following example, if data packets match any of mpls experimental values (0, 2, 5), the packets will be considered matching the rule of "class-map a1".

```
class-map a1
match mpls experimental 0 2 5
```

Related commands

Command	Description
N/A	N/A

Platform description	N/A

match qos-group

This command configures the class-map to use the group value of packets as the match rule. Use **no** form of this command to disable the configuration.

match qos-group { *group-value* }

no match qos-group { *group-value* }

Parameter description

Parameter	Description
group-value	The group value to be matched (range: 0-1023).

Default	By default, no match rule is configured by the system.
Command mode	Class-map interface configuration mode
Usage guidelines	The user can use this command to configure the class-map to use group value of data packets as the match rule. If the value is matched, the packets will be put into the corresponding CBWFQ queue. The group value of data packets is set through the action of "set qos-group" in class map. By default, the group value of all packets is 0.

Examples	Example 1: In the following example, if data packets match the group value of 2, the packets will be considered matching the rule of "class-map a1".
	`class-map a1`
	`match qos-group 2`

Related commands

Command	Description
set qos-group	Set the group value of packets.

Platform description	N/A

police

This command will configure committed access rate (CAR) in the policy-map and then apply to the interface through service-policy command. Use **no** form of this command to restore to default setting.

police cir *bps* { **pir** *bps* } *burst-normal burst-max*
conform-action *conform-action* **exceed-action** *exceed-action* {
violate-action *violate-action*}

no police cir *bps* { **pir** *bps* } *burst-normal burst-max*
conform-action *conform-action* **exceed-action** *exceed-action*
{**violate-action** *violate-action*}

Parameter description

Parameter	Description
cir	Maximum data rate of the traffic desired by the user (unit: bps).
pir	Peak data rate of the traffic desired by the user (unit: bps).
burst-normal	Size of token bucket (unit: bytes).
burst-max	Size of token bucket (unit: bytes).
conform-action	Action to take on traffic whose rate is less than the preset limit.
exceed-action	Action to take on traffic whose rate is above the preset limit.
violate-action	Action to take on traffic whose rate exceeds the preset limit for the second token bucket in the case of two token buckets system.
Action: action to take on packets, including:	
drop	Drop the packets
set-qos-transmit	Set the group value and send the packet
set-mpls-exp-transmit	Set the mpls experimental field and send the packet
transmit	Send this packet

Default By default, no "police" command is configured in policy-map.

Command mode	Policy-map class interface configuration mode.
Usage guidelines	See *QoS command Reference*.

Examples	Example 1: The following example creates a policy map named "policy1" and uses a class map in this policy map. The class map of "class1" limits the data rate of traffic with mpls experimental value being 6, and sets the mpls experimental value of traffic falling within CIR to 7.
	`class-map match-all a1`
	`match mpls experimental 6`
	`!`
	`policy-map policy`
	`class a1`
	`police cir 8000 2000 2000 conform-action set-mpls-exp-transmit 7 exceed-action drop`
	`!`
	`interface FastEthernet 1/0`
	`ip ref`
	`ip address 192.168.20.3 255.255.255.0`
	`mpls ip`
	`service-policy output policy`
	`!`

Related commands

Command	Description
N/A	N/A

Platform description	N/A

priority-list protocol

Use "**priority-list protocol**" command in global configuration mode to create the classifying rule, and assign packets to the specified priority queue according to the protocol type. Use **no** form of this command to delete the corresponding classifying rule.

priority-list *list-number* **protocol mpls** { **high** | **medium** | **normal** | **low** } **experimental** *exp-value*

no priority-list *list-number* **protocol mpls** { **high** | **medium** | **normal** | **low** } **experimental** *exp-value*

Parameter description

Parameter	Description
list-number	Any integer from 1 to 16 that identifies the priority queue list.
exp-value	The experimental value to be matched (range: 0-7).

Default

No queueing priorities.

Command mode

Global configuration mode.

Usage guidelines

When multiple rules are configured, the system will read the rules and match packets in the specified order. When a match is found, the system will stop searching and assign the packet to the appropriate queue.

Examples

Example 1: The following example configures the priority queue list of 2 and assigns all packets with protocol type being MPLS and EXP being 1 to the high priority queue.

```
Ruijie(config)# priority-list 2 protocol mpls high experimental 1
```

Related commands

Command	Description
priority-group	Apply the priority list to the interface.
priority-list default	Assign a default priority queue for those packets that do not match any other rule in the customized priority list.

Platform description

N/A

queue-list protocol

Use "**queue-list protocol**" command in global configuration mode to create the classifying rule, and assign packets to a specified customized queue according to the protocol type. Use **no** form of this command to delete the corresponding classifying rule.

queue-list *list-number* **protocol mpls** *queue-num* **experimental** *exp-value*

no queue-list *list-number* **protocol mpls** *queue-num* **experimental** *exp-value*

Parameter description

Parameter	Description
list-number	Any integer from 1 to 16 that identifies the queue list.
queue-num	Number of the queue. Any integer from 0 to 16.
exp-value	The experimental value to be matched (range: 0-7).

Default

No customized queueing priorities.

Command mode

Global configuration mode.

Usage guidelines

When multiple rules are configured, the system will read the rules and match packets in the specified order. When a match is found, the system will stop searching and assign the packet to the appropriate queue.

Examples

Example 1: The following example configures the customized queue list2 and assigns all packets with protocol type being MPLS and EXP being 1 to the customized queue4.

```
Ruijie(config)# queue-list 2 protocol mpls 4 experimental 1
```

Related commands

Command	Description
custom-queue-list	Apply the customized list to the interface

Platform description

N/A

random-detect experimental

This command configures experimental-classified traffic congestion avoidance related thresholds. Use **no** form of this command to restore to the default thresholds.

random-detect experimental *exp-value min-threshold max-threshold mark-prob-denominator*

no random-detect experimental *exp-value min-threshold max-threshold mark-prob-denominator*

Parameter description

Parameter	Description
exp-value	Experimental value; the traffic is classified according to this value.
min-threshold	The minimum drop threshold; the default value differs from traffic to traffic.
max-threshold	The maximum drop threshold; the default value differs from traffic to traffic.
mark-prob-denominator	Drop probability; the default value is 10, i.e., 1/10. The larger this value is, the smaller the drop probability will be.

Default

By default, you can execute "**show queue interface**" command to display the experimental-classified traffic congestion avoidance related thresholds.

Command mode

Interface configuration mode or Policy-map class interface configuration mode.

Usage guidelines

After configuring experimental-classified traffic congestion avoidance, each class of experimental traffic will have its default drop threshold and drop probability. The user can execute "random-detect experimental" command to redefine the drop threshold and drop probability of each class of experimental traffic.

Examples

Example 1: The following example configures experimental-classified congestion avoidance on the egress interface and resets the drop threshold and drop probability of each class of traffic with experimental value being 1, 2, 3 and 4 respectively.

```
interface Serial 1/0
ip ref
ip address 192.168.20.3 255.255.255.0
mpls ip
random-detect mpls-exp-base
```

```
random-detect experimental 1 5 100 10
random-detect experimental 2 10 100 10
random-detect experimental 3 20 100 10
random-detect experimental 4 30 100 10
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

random-detect mpls-exp-based

This command enables congestion avoidance which can be based on the EXP value of MPLS packets. Use **no** form of this command to restore to the default setting.

random-detect mpls-exp-based

no random-detect mpls-exp-based

Parameter description

Parameter	Description
N/A	N/A

Default

By default, the system will not apply any interface congestion avoidance policy to the network interface.

Command mode

Interface configuration mode or Policy-map class interface configuration mode.

Usage guidelines

WRED avoids the global TCP synchronization by randomly dropping packets. Thus, while the sending rates of some TCP sessions slow down after their packets are dropped, other TCP sessions remain at high sending rates. As there are always TCP sessions at high sending rates, link bandwidth is efficiently utilized.

Examples

Example 1: The following example configures ip dscp based congestion avoidance policy on the egress interface.

```
interface Serial1/0
ip ref
ip address 192.168.20.3 255.255.255.0
```

	`mpls ip` `random-detect mpls-exp-based`

Related commands	**Command**	**Description**
	N/A	N/A

Platform description	N/A

rate-limit

This command configures committed access rate (CAR) on the network interface. Use **no** form of this command to restore to the default setting.

rate-limit { **input** | **output** } [**access-group** *acl-index* | **dscp** *dscp-value* | **qos-group** *group-value*] *bps burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

no rate-limit { **input** | **output** } [**access-group** *acl-index* | **dscp** *dscp-value* | **qos-group** *group-value*] *bps burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*

Parameter description	**Parameter**	**Description**
	Input|*output*	The input or output traffic to be limited by the user.
	bps	Maximum data rate of the traffic desired by the user (unit: bps).
	group-value	The traffic matching this group ID will be limited (range: 0-99).
	Burst-normal burst-max	Size of token bucket (unit: bytes).
	Conform-action	Action to take on traffic whose rate is less than the preset limit.
	Exceed-action	Action to take on traffic whose rate is above the preset limit.
	Action: action to take on packets, including:	
	drop	Drop the packets

set-mpls-exp-continue	After setting mpls experimental field, this packet continues to match the next policy
set-mpls-exp-transmit	Set the mpls experimental field and send the packet
set-qos-continue	After setting the group ID, this packet continues to match the next policy
set-qos-transmit	Set the group value and send the packet

Default

By default, the system will not apply any interface rate-limit to the network interface.

Command mode

Interface configuration mode.

Usage guidelines

See *QoS command Reference*.

Examples

Example 1: The following example configures CAR traffic supervision on the ingress interface and sets mpls experimental to 2.

```
interface FastEthernet 1/0
ip ref
ip address 192.168.20.3 255.255.255.0
mpls ip
rate-limit input 8000 2000 2000 conform-action set-mpls-exp-transmit 2 exceed-action drop
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

set cos

This command configures precedence value marking of the COS field for traffic corresponding to class map as used by the policy map. Use **no** form of this command to restore to default setting.

set cos { *cos-value* **|** [**dscp | precedence | qos-group** [**table** *table-map name*]] }

no set cos { *cos-value* **|** [**dscp | precedence | qos-group** [**table** *table-map name*]] }

Parameter description

Parameter	Description
cos-value	Set cos value (range: 0-7).
table-map name	Name of table-map to be used.

Default

By default, this command isn't applied to the policy map.

Command mode

Policy-map class interface configuration mode.

Usage guidelines

1. Configure cos-value. When a match is found, set the COS field of Ethernet packet to cos-value.

2. Configure dscp. When a match is found, set the COS field of Ethernet packet to class value in dscp field of ip packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in dscp field of ip packet, and the cos field of Ethernet packet will be set to the to-value.

3. Configure precedence. When a match is found, set the COS field of Ethernet packet to class value in precedence field of ip packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in precedence field of ip packet, and the cos field of Ethernet packet will be set to the to-value.

4. Configure qos-group. When a match is found, set the cos field of Ethernet packet to qos-group ID of the packet. If table-map is also configured, to-value will be looked up in the table-map using the qos-group value of packet, and the cos field of Ethernet packet will be set to the to-value.

Examples

Example 1: The following example sets cos value of all packets matching class map "class1" in the policy map of "policy1" to 3.

```
policy-map policy1
class class1
```

```
set cos 3
```

Example 1: The following example sets cos value of all packets matching class map "class1" in the policy map of "policy1" to dscp value.

```
policy-map policy1
class class1
set cos dscp
```

Example 3: The following example sets cos value of all packets matching class map "class1" in the policy map of "policy1" to the to-value of dscp as found in tablemap1.

```
policy-map policy1
class class1
set cos dscp table tablemap1
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

set dscp

This command configures dscp value of the TOS field for traffic corresponding to class map as used by the policy map. Use **no** form of this command to restore to default setting.

set dscp { *dscp-value* **|** [**experimental | qos-group** [**table** *table-map name*]] }

no set dscp { *dscp-value* **|** [**experimental | qos-group** [**table** *table-map name*]] }

Parameter description

Parameter	Description
dscp-value	Set dscp value (range: 0-63).
table-map name	Name of table-map to be used.

Default By default, this command isn't applied to the policy map.

Command mode Policy-map class interface configuration mode.

Usage guidelines

1. Configure dscp-value. When a match is found, set the dscp field of ip packet to dscp-value.
2. Configure experimental. When a match is found, set the

dscp field of IP packet to class value in exp field of mpls packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in exp field of mpls packet, and the dscp field of ip packet will be set to the to-value.

3. Configure qos-group. When a match is found, set the dscp field of ip packet to qos-group ID of the packet. If table-map is also configured, to-value will be looked up in the table-map using the qos-group value of packet, and the dscp field of ip packet will be set to the to-value.

Examples

Example 1: The following example sets ip dscp value of all packets matching class map "class1" in the policy map of "policy1" to 32.

```
policy-map policy1
class class1
set dscp 32
```

Example 2: The following example sets ip dscp value of all packets matching class map "class1" in the policy map of "policy1" to mpls exp value.

```
policy-map policy1
class class1
set dscp experimental
```

Example 3: The following example sets ip dscp value of all packets matching class map "class1" in the policy map of "policy1" to the to-value of mpls experimental as found in tablemap1.

```
policy-map policy1
class class1
set dscp experimental table tablemap1
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

set mpls experimental

This command configures experimental value of the mpls field for traffic corresponding to class map as used by the policy map. Use **no** form of this command to restore to default setting.

set mpls experimental { *exp-value* **|** [**dscp | precedence | qos-group** [**table** *table-map name*]] }

no set mpls experimental { *exp-value* **|** [**dscp | precedence | qos-group** [**table** *table-map name*]] }

Parameter description

Parameter	Description
exp-value	Set experimental value (range: 0-7).
table-map name	Name of table-map to be used.

Default

By default, this command isn't applied to the policy map.

Command mode

Policy-map class interface configuration mode.

Usage guidelines

1. Configure exp-value. When a match is found, set the experimental field of mpls packet to exp-value.

2. Configure dscp. When a match is found, set the experimental field of mpls packet to class value in dscp field of ip packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in dscp field of ip packet, and the experimental field of mpls packet will be set to the to-value.

3. Configure precedence. When a match is found, set the experimental field of mpls packet to precedence value of ip packet. If table-map is also configured, to-value will be looked up in the table-map using the precedence value of ip packet, and the experimental field of mpls packet will be set to the to-value.

4. Configure qos-group. When a match is found, set the experimental field of mpls packet to qos-group ID of the packet. If table-map is also configured, to-value will be looked up in the table-map using the qos-group ID of packet, and the experimental field of mpls packet will be set to the to-value.

Examples

Example 1: The following example sets mpls experimental value of all packets matching class map "class1" in the policy map of "policy1" to 5.

```
policy-map policy1
class class1
set mpls experimental 5
```

Example 2: The following example sets mpls experimental value of all packets matching class map "class1" in the policy map of "policy1" to ip dscp value.

```
policy-map policy1
class class1
set mpls experimental dscp
```

Example 3: The following example sets mpls experimental value of all packets matching class map "class1" in the policy map of "policy1" to the to-value of ip dscp as found in tablemap1.

```
policy-map policy1
class class1
set mpls experimental dscp table tablemap1
```

Example 4: The following example sets mpls experimental value of all packets matching class map "class1" in the policy map of "policy1" to ip precedence value.

```
policy-map policy1
class class1
set mpls experimental precedence
```

Example 5: The following example sets mpls experimental value of all packets matching class map "class1" in the policy map of "policy1" to the to-value of ip precedence as found in tablemap1.

```
policy-map policy1
class class1
set mpls experimental precedence table tablemap1
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

set precedence

This command configures dscp value of the TOS field for traffic corresponding to class map as used by the policy map. Use **no** form of this command to restore to default setting.

set precedence { *prec-value* **|** [**experimental | qos-group** [**table** *table-map name*]] }

no set precedence { *prec-value* **|** [**experimental | qos-group** [**table** *table-map name*]] }

Parameter

Parameter	Description

description

prec-value	Precedence value to be matched
table-map name	Name of table-map to be used.

Default

By default, this command isn't applied to the policy map.

Command mode

Policy-map class interface configuration mode.

Usage guidelines

1. Configure prec-value. When a match is found, set the precedence field of ip packet to prec-value.

2. Configure experimental. When a match is found, set the precedence field of IP packet to class value in exp field of mpls packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in exp field of mpls packet, and the precedence field of ip packet will be set to the to-value.

3. Configure qos-group. When a match is found, set the precedence field of ip packet to qos-group ID of the packet. If table-map is also configured, to-value will be looked up in the table-map using the qos-group ID of packet, and the precedence field of ip packet will be set to the to-value.

Examples

Example 1: The following example sets precedence value of all packets matching class map "class1" in the policy map of "policy1" to 5.

```
policy-map policy1
class class1
set precedence 5
```

Example 2: The following example sets ip precedence value of all packets matching class map "class1" in the policy map of "policy1" to mpls experimental value.

```
policy-map policy1
class class1
set precedence experimental
```

Example 3: The following example sets ip precedence value of all packets matching class map "class1" in the policy map of "policy1" to the to-value of mpls experimental as found in tablemap1.

```
policy-map policy1
class class1
```

```
set precedence experimental table tablemap1
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

set qos-group

This command configures group ID for traffic corresponding to class map as used by the policy map. Use **no** form of this command to restore to default setting.

set qos-group { *group-value* **|** [**dscp | precedence | mpls experimental | cos** [**table** *table-map name*]] }

no set qos-group { *group-value* **|** [**dscp | precedence | mpls experimental | cos** [**table** *table-map name*]] }

Parameter description

Parameter	Description
group-value	Configure the group ID (range: 0-1023).
table-map name	Name of table-map to be used.

Default By default, this command isn't applied to the policy map.

Command mode Policy-map class interface configuration mode.

Usage guidelines

1. Configure group-value. When a match is found, set the group ID of packet to group-value.
2. Configure dscp. When a match is found, set the group ID of packet to class value in dscp field of ip packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in dscp field of ip packet, and the group ID of packet will be set to the to-value.
3. Configure precedence. When a match is found, set the group ID of packet to class value in precedence field of ip packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in precedence field of ip packet, and the group ID of packet

will be set to the to-value.

4. Configure experimental. When a match is found, set the group ID of packet to class value in exp field of mpls packet. If table-map is also configured, to-value will be looked up in the table-map using the class value in exp field of mpls packet, and the group ID of packet will be set to the to-value.

5. Configure cos. When a match is found, set the group ID of packet to cos value of Ethernet packet. If table-map is also configured, to-value will be looked up in the table-map using the cos value of Ethernet packet, and the group ID of packet will be set to the to-value.

Examples

Example 1: The following example sets group ID of all packets matching class map "class1" in the policy map of "policy1" to 5.

```
policy-map policy1
class class1
set qos-group 5
```

Example 2: The following example sets qos-group ID of all packets matching class map "class1" in the policy map of "policy1" to mpls experimental value.

```
policy-map policy1
class class1
set qos-group experimental
```

Example 3: The following example sets qos-group ID of all packets matching class map "class1" in the policy map of "policy1" to the to-value of dscp as found in tablemap1.

```
policy-map policy1
class class1
set qos-group dscp table tablemap1
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

table-map

Use this command to enter the configuration mode of the specified table-map. If the specified table-map doesn't exist, the system will create a table-map using the specified

name. Use **no** form of this command to remove the table-map with the specified name from the system.

table-map *table-map-name*

no table-map *table-map-name*

Parameter description

Parameter	Description
table-map-name	Name of table-map. It is also an identifier in the system. The name can be a maximum of 127 characters.

Default

By default, no class map is configured by the system.

Command mode

Global configuration mode.

Usage guidelines

Table-map command allows the user to create the specified table-map and enter table-map interface configuration mode. On the table-map interface, the user can map one value to another value as needed.

When table-map is used, it cannot be removed.

Examples

Example 1: The following example configures a table-map named "tablemap1".

```
table-map tablemap1
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

show table-map

Execute "**show table-map**" command to display the configuration of a specified table-map or all table-maps.

show table-map [*table-map-name*]

Parameter description

Parameter	Description
table-map-name	Name.

Default	NA
Command mode	Privileged EXEC mode
Usage guidelines	The user can use this command to display relevant information about table-map. Description of information displayed: Table Map *table-map-name* from value range(*value-range*), to value range(*value-range*) map from *from-value* to *to-value* …… default *default- behavior* **Parameter description:** *table-map-name:* name of table-map *value-range:* value range *from-value:* Map-from value *to-value:* Map-to value *default- behavior:* Default behavior of table-map, i.e., copy

Examples	Assuming that the following configurations are used:
	!
	table-map tablemap1
	map from 3 to 2
	default 7
	!
	Example 1 displays the relevant information about the table-map named tablemap1.
	`Ruijie(config)#show table-map tablemap1`
	`Table Map tablemap1`
	`from value range(0 - 99), to value range(0 - 99)`
	`map from 3 to 2`
	`default 7`
	`quote count 0`

Related commands	**Command**	**Description**
	N/A	N/A

Platform description	N/A

IP Multicast Commands

IPv4 Multicast Commands

clear ip mroute

Use this command to remove the forwarding information of the IP multicast routes.

clear ip mroute [**vrf** *vrf-name*] { * | *group-address* [*source –address*] }

Parameter Description

Parameter	Description
vrf vrf-name	Specifies the VRF instance.
*	Removes all forwarding information in the IP multicast route table.
group-address	Group IP address of IP multicast routes
source-address	Source IP address of IP multicast routes

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example removes the entries whose group IP address is 230.0.0.1 from the multicast route 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 The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

clear ip mroute statistics

Use this command to remove the statistics of IP multicast routes.

clear ip mroute [**vrf** *vrf-name*] **statistics** { ***** | *group-address* [*source –address*] }

Parameter Description

Parameter	Description

vrf *vrf-name*	Specifies the VRF instance.
*	Removes all forwarding entries in the IP multicast route table.
group-address	Group IP address of IP multicast routes
source-address	Source IP address of IP multicast routes

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to remove the statistics of IP multicast routes.

Configuration Examples The following example removes the statistics of entries whose group IP address is 230.0.0.1 from the multicast route 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	Removes the multicast route forwarding information.

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip mroute

Use this command to configure static multicast routes.
Use the **no** form of this command to delete the configured routes.
ip mroute [**vrf** *vrf-name*] *source-address mask* { **fallback-lookup** { **global** | **vrf** *vrf-name* } | [*protocol*] { *rpf-addrress* | *interface-type interface-number* } } [*distance*]
no ip mroute [**vrf** *vrf-name*] *source-address mask* [*protocol*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.
source-address	Source IP address of the multicast route
mask	Mask of the source IP address
fallback-lookup { **global**	**vrf** *vrf-name* }	VRF used for RPF lookup
protocol	(Optional) Unicast routing protocol being used
rpf-address	Incoming interface of the multicast route
interface-type	Interface type and interface ID

interface-number	
distance	Management distance used to determine whether to use the route for RPF routing. Its range is from 1 to 255. The default value is 0.

Defaults The default value of *distance* is 0.

Command Mode Global configuration mode

Usage Guide The route configured by using this command is for the purpose of RFF check. Note that the configured route is prior to the route learned from the unicast route protocol.
If the outgoing direction of the static multicast route but not the next-hop IP address shall be specified, the outgoing direction must be of the point-to-point type.
The RPF rule is as follows:
Select a best multicast route from the multicast list. (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. Then compare the mask length of the best multicast and unicast routes. The one with the greater mask length is used as the RPF route. If the mask length is the same, compare the distance. The one with the smaller distance is used as the RPF route. If the distance is the same, the multicast route is used as the RPF route.

Configuration Examples The following example allows the multicast routes of all 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip multicast boundary

Use this command to configure the boundary of an IP multicast group.
Use the **no** form of this command to remove the configured boundary.
ip multicast boundary *access-list* [**in** | **out**]
no ip multicast boundary *access-list* [**in** | **out**]

Parameter Description

Parameter	Description
access-list	Access list associated with the multicast boundary

in	Indicates that the multicast boundary applies to the incoming direction of the multicast flow.
out	Indicates that the multicast boundary applies to the outgoing direction of the multicast flow.

Defaults The boundary of a specified IP multicast group is configured by default.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the boundary of a specified IP multicast group. Note that the ACL associated with the multicast boundary can be either standard ACL or extended ACL. But the extended ACL only matches the destination IP address.


Caution

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 standard 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

no ip multicast [**vrf** *vrf-name*] **route-limit**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.
limit	Number of the entries that can be added to the multicast routing table. Its range is from 1 to 2147483647. The default value is 1024.

threshold	(Optional) Number of multicast routes at which alarms will be generated. The default value is 2147483647.

Defaults The default value of *limit* is 1024.
The default value of *threshold* is 2147483647.

Command Mode Global configuration mode

Usage Guide Use this command to limit the number of entries that can be added to the IPv4 multicast routing table.

The hardware resources of different devices are limited. The routes exceeding the hardware resource limit will be forwarded by software, which deteriorates device performance.

Configuration Examples The following example sets the maximum number of entries that can be added to the IPv4 multicast routing table to 500.

```
Ruijie(config)# ip multicast route-limit 500
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip multicast-routing

Use this command to enable multicast routing forwarding.
Use the **no** form of this command to disable the function.
ip multicast-routing [**vrf** *vrf-name*]
no ip multicast-routing [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults Multicast routing forwarding is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable IPv4 multicast routing forwarding. If IPv4 multicast routing forwarding is disabled, the multicast protocol cannot be enabled.


Note

It is not recommended to configure different v4 multicast routing protocols on different interfaces of a device.

Configuration Examples This following example enables multicast routing forwarding.

```
Ruijie(config)# ip multicast-routing
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip multicast ttl-threshold

Use this command to configure the TTL (time-to-live) threshold on the interface.
Use the **no** form of this command to restore it to the default value.
ip multicast ttl-threshold *ttl-value*
ip multicast ttl-threshold

Parameter Description

Parameter	Description
ttl-value	TTL threshold on the interface, in the range of 0 to 255

Defaults The default value of *ttl-value* is 0.

Command Mode Interface configuration mode

Usage Guide A device with multicast enabled can maintain a TTL threshold for every interface. If the TTL of the multicast packet received is greater than the TTL threshold of the interface, the packet will be forwarded. Otherwise, the packet is discarded. Note that the TTL threshold is effective only to the multicast frames, and 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
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

ip multicast rpf longest-match

Use the RPF rule to select the static multicast route, MBGP route, and unicast route for the purpose of RPF check from the static multicast route list, MBGP route list, and unicast route list respectively. Use this command to select the route with the longest-matched mask from the above-mentioned three routes. If the priority values of these three routes are the same, the route will be selected in the following sequence: static multicast route -> MBGP route -> unicast route.

Use the **no** form of this command to restore the default setting. By default, the route with the highest priority is selected from the above-mentioned three routes. If the priority values of these three routes are the same, the route will be selected in the following sequence: static multicast route -> MBGP route -> unicast route.

ip multicast [**vrf** *vrf-name*] **rpf longest-match**

no ip multicast [**vrf** *vrf-name*] **rpf longest-match**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults Use the RPF rule to select the static multicast route, MBGP route, and unicast route for the purpose of RPF check from the static multicast route list, MBGP route list, and unicast route list.

The route with the highest priority is selected from the above-mentioned three routes. If the priority values of these three routes are the same, the route will be selected in the following sequence: static multicast route -> MBGP route -> unicast route.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures to select the route with the longest-matched mask.

```
Ruijie(config)# ip multicast rpf longest-match
```

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip multicast rpf proxy

ip multicast [**vrf** *vrf-name*] **rpf proxy** [**rd**] { **vector | disable** }

Parameter

Parameter	Description

Description

vrf *vrf-name*	Specifies the VRF.
rd	Only when the VRF keyword is specified, the RPF Vector of the RD can be determined whether to be carried.
vector	Specifies whether to carry the RPF Vector.
disable	Disables the function of receiving the RPF Vector.

Defaults The RPF Vector is disabled and receiving the RPF Vector is allowed by default.

Command Mode Global configuration mode

Usage Guide

■ Introduction to the proxy

To make the PIM-SM send the Join packet with RPF Vector to create the SPT, run the **ip multicast** [**vrf** *vrf-name*] **rpf proxy** [**rd**] **vector** command, which is used for creating the SPT across the AS. With this command configured, the PIM-SIM will query a proxy address to the multicast source. The PIM-SIM will use this proxy address as the destination address to search the RPF neighbor and send the Join packets to this RPF neighbor. At the same time, the PIM-SM will also put this proxy address into the Join packets, so that the RPF neighbor can also perform the RPF detection.

In the OptionB's across-domain VPAN deployment environment, the PE will select the next hop of the BGP MDT address family routes as the proxy. This MDT route is created by the PE for each multicast VPN. In the OptionC deployment environment, the PE will select the next hop of the BGP unicast route as the proxy. The is because, in the OptionB environment, there may be no routes to other AS-PEs in the PE; while in the OptionC deployment environment, there exists the BGP route to other AS-PE in the PE, so that the PE can directly use the next hop of this BGP route as the proxy. For the commands related to the BGP MDT address family, refer to the *BGP4 commands guide.*

■ RPF Vector configuration guide

To enable the RPF Vector in the OptionB environment, run the **ip multicast** [**vrf** *vrf-name*] **rpf proxy rd vector** command to enable the carrying of the **rd** parameter. After the configuration, the RD information will be placed into the Join packets. The ASBR will change the next hop of the MDT route in the OptionB environment. If there are multiple VPNs on a PE, the multiple MDT routes sent by this PE may have different next hops due to the next hop change, and these routes cannot be distinguished even though the PE address is used as the index separately. In this case, the RD must be used with the PE address to distinguish different MDT routes, so as to select a proxy address for each VPN. If the **vrf** parameter is configured, the public network SPT created by the VPN corresponding to the vrf-name will enable the RPF Vector.

To enable the RPF Vector in the OptionC environment, run the **ip multicast rpf proxy vector** command. In this case, the Join packets carry the proxy address rather than the RD information.

To disable the RPF Vector, run the **ip multicast rpf proxy disable** command. After the configuration, the PIM-SM will discard the RPF Vector information in the Join packets. If the **vector** and **disable** parameters are configured at the same time, the PIM-SM can still enable the RPF Vector.

Configuration Examples

```
Ruijie (config)# ip multicast rpf proxy vector
```

Related Commands	Command	Description
	N/A	N/A

Platform Description This command is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip mroute

Use this command to display the multicast forwarding table.

show ip mroute [**vrf** *vrf-name*] [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]

Parameter Description

Parameter	Description
vrf v*rf-name*	Specifies the VRF instance.
group-or-source-address	Multicast or source IP address
group-or-source-address	Multicast or source IP address. The two addresses in this command cannot be the multicast addresses or source addresses at the same time.
dense	Displays the PIM-DM multicast core table.
sparse	Displays the PIM-SM multicast core table.
summary	Displays the summary of the multicast routing table.
count	Displays the count of the multicast routing table.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

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 the entry 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 co nt,,	Forwarding count: count of packets or bytes 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	Enables the multicast routing forwarding.
ip pim dense-mode	Enables the PIM-DM on the interface.
ip pim sparse-mode	Enables the PIM-SM on the interface.

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip mroute static

Use this command to display the IPv4 static multicast routing information.

show ip mroute [**vrf** *vrf-name*] **static**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the static multicast route. In the same conditions, the priority of the static multicast route is higher than the dynamically learned route.

Configuration Examples The following example displays the information of the static multicast routing information.

```
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 static multicast routing (including VRF information).

```
Ruijie# show ip mroute static
Mroute: 172.16.0.0, VRF: vpn1, distance: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip rpf

Use this command to display the RPF information of the specified source IP address.

show ip rpf [**vrf** *vrf-name*] { *source-address* [*group-address*] [**rd** *route-distinguisher*] } [**metric**]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.
source-address	Specified source IP address
group-address	Specified group IP address
rd *route-distinguisher*	Uses the RD proxy for the search.
metric	Displays the metric of the MDT-SAFI route.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

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
```

Related Commands

Command	Description
N/A	N/A

Platform Description Parameters, such as **vrf**, **group-address**, **rd**, and **metric**, are supported only on RSR20, RSR30, RSR50, and RSR50E.

show ip mvif

Use this command to display the basic information of the multicast interface.

show ip mvif [**vrf** *vrf-name*] { *interface-type interface-number* }

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.
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 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
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip mrf mfc

Use this command to display the IPv4 multicast routing forwarding table.

show ip mrf [**vrf** *vrf-name*] **mfc** [*source-address group-address*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Private network's VRF name. If no vrf name is specified, the public network's multicast routing forwarding entries are displayed by default.
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 or group address are specified, all mfc entries are displayed.
- When the only source address and group address are specified, 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 output 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 specifies 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	Indicates whether the entry has been

	configured on the next layer forwarding table.
MIN_MTU MTU	Minimum MTU of the entry
MIN_MTU_IFINDEX	Interface index with the minimum MTU value
WRONG IF	Statistics 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 VLAN 3. 1 is the ttl threshold of this layer-3 interface.

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug nsm mcast all

Use this command to turn on all multicast debugging switches.
Use the **no** form of this command to turn off all the debugging switches.
debug nsm mcast [**vrf** *vrf-name*] **all**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults All multicast debugging switches are disabled by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to turn on all multicast debugging switches. In this way, you can check related running process.

Configuration Examples The following example turns on all the multicast debugging switches.

```
Ruijie# debug nsm mcast all
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug nsm mcast fib-msg

Use this command to turn on the fib-msg debugging switch.
Use the **no** form of this command to turn off the debugging switch.
debug nsm mcast [**vrf** *vrf-name*] **fib-msg**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults The fib-msg debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to turn on the fib-msg debugging switch. In this way, you can check the fib-msg running process.

Configuration Examples The following example turns on the fib-msg debugging switch.

```
Ruijie# debug nsm mcast fib-msg
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug nsm mcast register

Use this command to turn on the register debugging switch.
Use the **no** form of this command to turn off the debugging switch.
debug nsm mcast [**vrf** *vrf-name*] **register**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults The register debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to turn on the register debugging switch. In this way, you can check the processing of the register interface and register packets of the multicast core.

Configuration Examples The following example turns on the register debugging switch.

```
Ruijie# debug nsm mcast register
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug nsm mcast stats

Use this command to turn on the interface statistics debugging switch.
Use the **no** form of this command to turn off the debugging switch.
debug nsm mcast [**vrf** *vrf-name*] **stats**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults The interface statistics debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to turn on the interface statistics debugging switch. In this way, you can check the processing of interface and performance statistics of the multicast core.

Configuration Examples The following example turns on the interface statistics debugging switch.

```
Ruijie# debug nsm mcast stats
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug nsm mcast vif

Use this command to turn on the VIF debugging switch.
Use the **no** form of this command to turn off the debugging switch.
debug nsm mcast [**vrf** *vrf-name*] **vif**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults The VIF debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to turn on the VIF debugging switch. In this way, you can check the interface running process of the multicast core.

Configuration Examples The following example turns on the VIF debugging switch.

```
Ruijie# debug nsm mcast vif
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug nsm mcast mrt

Use this command to turn on the MRT debugging switch.
Use the **no** form of this command to turn off the debugging switch.
debug nsm mcast [**vrf** *vrf-name*] **mrt**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF instance.

Defaults The MRT debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to turn on the MRT debugging switch. In this way, you can check the multicast routing information of the multicast core.

Configuration Examples The following example turns on the MRT debugging switch.

```
Ruijie# debug nsm mcast mrt
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug ip mrf forwarding

Use this command to turn on the debugging switch to check the operation of IPv4 multicast forwarding.

Use the **no** form of this command to turn off the debugging switch.

debug ip mrf [**vrf** *vrf-name*] **forwarding**

no debug ip mrf [**vrf** *vrf-name*] **forwarding**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the private network's VRF of which the debugging information is to be checked.

Defaults This debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example turns on the debugging switch to check the operation of forwarding IPv4 multicast messages.

```
Ruijie# debug ip mrf forwarding
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug ip mrf mfc

Use this command to turn on the debugging switch to check the processing of IPv4 multicast routing forwarding entries.
Use the **no** form of this command to turn off the debugging switch.
debug ip mrf [**vrf** *vrf-name*] **mfc**
no debug ip mrf [**vrf** *vrf-name*] **mfc**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the private network's VRF of which the debugging information is to be checked.

Defaults This debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example turns on the debugging switch to check the processing of IPv4 multicast routing forwarding entries.

```
Ruijie# debug ip mrf mfc
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

debug ip mrf event

Use this command to turn on the debugging switch to check the processing of IPv4 multicast routing forwarding events.
Use the **no** form of this command to turn off the debugging switch.
debug ip mrf [**vrf** *vrf-name*] **event**
no debug ip mrf [**vrf** *vrf-name*] **event**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the private network's VRF of which the debugging information is to be checked.

Defaults This debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example turns on the debugging switch to check the processing of IPv4 multicast routing forwarding events.

```
Ruijie# debug ip mrf event
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

IPv6 Multicast Commands

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

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.

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
mask	Mask of the source IPv6 address
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.

Defaults 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
```

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

Defaults The boundary of a specified IPv6 multicast group is not defined by default.

Command Mode Interface configuration mode

Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IPv6 address.

Usage Guide

This command filters MLD, PIM-SMv6 packets of the specified IPv6 address range. Multicast packets will not be received and sent through the interface of the boundary.

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
```

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 2147483647
threshold	(Optional) Number of IPv6 multicast routes at which alarms will be triggered

Defaults

The default value of *limit* is 1024.
The default value of *threshold* is 2147483647.

Command Mode

Global configuration mode

This command is used to restrict the number of route adding to the IPv6 multicast table.

Usage Guide

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
```

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

Defaults This function is disabled by default

Command Mode Global configuration mode

Use this command to enable the IPv6 multicast routing forwarding. With this function disabled, the multicast protocol cannot be enabled.

Usage Guide

This command must be configured to enable the IPv6 multicast routing forwarding. This function conflicts with IGMP Snooping.

Configuration Examples

The following example enables the IPv6 multicast routing forwarding.

```
Ruijie(config)# ipv6 multicast-routing
```

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

Defaults

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
```

show ipv6 mroute

Use this command to display the IPv6 multicast forwarding table.
show ipv6 mroute [*group-or-source-address* [*group-or-source-address*]] [**sparse**] [**summary** | **count**]

Parameter Description

Parameter	Description
v6group-address	Multicat group IPv6 address
v6source-address	Multicast source IPv6 address
sparse	Displays the core entry of the multicast routing table.
summary	Displays the summary of the multicast routing table.
count	Displays the count of the multicast routing table.

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

The following example displays all information of the IPv6 multicast routing table.

```
Ruijie# show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SMv6, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example displays the count of the routing table.

```
Ruijie# show ipv6 mroute count
IPv6 Multicast Statistics
Total 1 routes using 168 bytes memory
Route limit/Route threshold: 1024/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 77/147/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 77/147/0
Immediate/Timed stat updates sent to clients: 0/29
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:09
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(2222::1234, ff56::1234), Forwarding: 1/0, Other: 0
 Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example displays the summary of the routing table.

```
Ruijie# show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), 00:00:28/00:03:25, PIM-SMv6, Flags: TF
```

	Command	Description
Related Commands	**clear ipv6 mroute**	N/A
	clear ipv6 mroute statistics	N/A

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/Global configuration mode/Interface configuration 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
```

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/Global configuration mode/Interface configuration 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
```

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/Global configuration mode/Interface configuration 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
```

IGMP Commands

ip igmp access-group

Use this command to control multicast groups on the interface.

Use the **no** form of this command to disable the function.

ip igmp access-group *access-list*

no ip igmp access-group

Parameter Description

Parameter	Description
access-list	Specifies name of an access control list (ACL). It can be numerics ranged from 1 to 199 or from 1300 to 2699. It can also be characters.

Defaults Filtering conditions are not set by default.

Command Mode Interface configuration mode

Usage Guide

You can add some interfaces of the host in a subnet to multiple multicast groups. You can use this command to control these multicast groups.

Caution When IGMPv3 is enabled, this command is associated with the extended ACL. When the received IGMP report information is (S1,S2,S3…Sn,G), this command will perform a matching check on the (0,G) information by using the corresponding ACL. Therefore, to use this command to properly filter (S1,S2,S3…Sn,G), an explicit (0,G) record must be configured for the extended ACL.

Configuration Examples

The following example enables the host service to add interface Eth0/1 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 interface Eth0/1 so that the interface processes only IGMP packets with the source address of 1.1.1.1 and group address of 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

ip igmp join-group

Use this command to add a certain interface of a device to a multicast group.
Use the **no** form of this command to remove the setting.
ip igmp join-group *group-address*
no ip igmp join-group *group-address*

Parameter Description

Parameter	Description
group-address	IP address of the multicast group to which the interface is to be added

Defaults The interface is not added to any multicast group by default.

Command Mode Interface configuration mode

Usage Guide Use this comand to enable the host activities on a certain interface of a device, so that the device can proactively learn the information of the corresponding group.

Configuration Examples The following example adds interface Eth0/1 of a device to group 233.3.3.3.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ip igmp join-group 233.3.3.3
Ruijie(config-if)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip igmp immediate-leave group-list

Use this command to shorten the delay of leaving a group in IGMPv2 and IGMPv3. This command can be used only when a single receiving host is connected to a single interface. Use the **no** form of this command to disable the function.
ip igmp immediate-leave group-list *access-list*
no ip igmp immediate-leave

Parameter Description

Parameter	Description
access-list	Name of the 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 sends a specific-group query message upon receiving the leave message from the interface. When the host response is timeout, the device stops forwarding packets to this interface. The timeout length depends on the last member query interval and IGMP robustness variable. The default value is 2 seconds.
If this command is configured, the device does not send a specific-group query message upon receiving the leave message from the interface. Instead, the device directly removes this interface from the IGMP buffer and notifies the IGMP protocol. This will shorten the time significantly.

Configuration Examples

The following example enables the immediate-leave function for some multicast groups. Ensure that each interface of these multicast groups has only one group member.

```
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
ip igmp last-member-query-interval	Last member query interval.

Platform Description N/A

ip igmp last-member-query-count

Use this command to configure the last member query count, which specifies the number of query packets that a multicast device sends continuously upon receiving the leave message. Use the **no** form of this command to restore the default value.
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 2 to 7

Defaults The default value of last member query count is 2.

Command Mode Interface configuration mode

Usage Guide When the device receives an IGMPv2 group leave message on an interface, the device waits for the duration of query interval multiplying the value of last-member-query-count. The device will delete member information about this group on the interface if no 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

ip igmp last-member-query-interval

Use this command to set the time interval of sending a specific-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 of sending specific-group query messages in the range from1 to 255. The unit is 1/10 second.

Defaults The time interval of sending specific-group query messages is 1 second by default.

Command Mode Interface configuration mode

Usage Guide When the device receives an IGMPv2 group leave message on an interface, the device waits for the duration of query interval multiplying the value of last-member-query-count. The device will delete member information about this group on the interface if no member report is received within the waiting time.

Configuration Examples

The following example sets the interval of sending specific-group query messages 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
ip igmp immediate-leave	Enables the immediate-leave function.

Platform Description

N/A

ip igmp limit (in interface configuration mode)

Use this command to set the maximum number of IGMP states on the interface.
Use the **no** form of this command to remove the setting.
ip igmp limit *number* [**except** *access-list*]
no ip igmp limit

Parameter Description

Parameter	Description
number	The maximum number of IGMP states. Its range varies with devices.
except	(Optional) Prevents the groups in the access list from taking part in calculation. These groups are not limited by the maximum number.
access-list	(Optional) Name of the access list

Defaults

The maximum number of IGMP states is 1024 by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command in global configuration mode to limit the number of IGMP group members. The messages of the members exceeding the limit are not recorded and processed.
This command can be configured globally or on a specific interface. The messages of the members exceeding the interface or global configuration will be ignored.

Configuration Examples

The following example sets the maximum number of IGMP states to 300.

```
Ruijie(config-if)# ip igmp limit 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip igmp limit (in global configuration mode)

Use this command to globally set the maximum number of IGMP group records.
Use the **no** form of this command to remove the setting.
ip igmp [**vrf** *vrf-name*] **limit** *number* [**except** *access-list*]
no ip igmp limit

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies a VRF.
number	The maximum number of IGMP states. Its range varies with devices.
except	(Optional) Prevents the groups in the access list from taking part in calculation. These groups are not limited by the maximum number.
access-list	(Optional) Name of the access list

Defaults The maximum number of IGMP group records is 65530 by default.

Command Mode Global configuration mode

Usage Guide Use this command to globally configure the maximum number of IGMP group records. The messages of the members exceeding the limit will not be saved in the IGMP buffer or forwarded. This command can be configured globally or on a specific interface. The messages of the members exceeding the interface or global configuration will be ignored.

Configuration Examples The following example sets the maximum number of IGMP group records to 300.

```
Ruijie(config) # ip igmp limit 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description The *vrf* parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

ip igmp mroute-proxy

Use this command to enable an interface to function as a mroute-proxy interface that can forward packets to its uplink interfaces.
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 a proxy-service interface, the interface can forward the IGMP packets sent by other members.

Configuration Examples The following example configures an interface as a 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

ip igmp proxy-service

Use this command to enable the service function of all downlink mroute-proxy interfaces. After you run this command on an interface, the interface becomes the uplink interface of the corresponding mroute-proxy and associates its downlink interfaces and maintains the group information reported by the downlink interfaces.

ip igmp proxy-service

no ip igmp proxy-service

Parameter Description	Parameter	Description
	N/A	N/A

Defaults All interfaces are not in the proxy-serice status by default.

Command Mode Interface configuration mode

Usage Guide This command can configure a maximum of 32 proxy-service interfaces on a device. The number of interfaces with IGMP Proxy enabled is limited by the number of supported multicast interfaces. Upon receiving a query message, the proxy-service interface responds according to

the IGMP group member information maintained by the interface itself. The member information maintained by the proxy-service interface is collected from the interface configured as mroute-proxy. Therefore, if an interface is configured as a proxy-service interface, the interface performs the host activities, but not the router activities.
If the switchport operation is performed on a proxy-service interface of a switch, the **ip igmp mroute-proxy interface** command configured on the associated downlink interfaces will be automatically deleted.

Configuration Examples

The following example configures an interface as a proxy-service module.

```
Ruijie(config-if)# ip igmp proxy-service
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip igmp query-interval

Use this command to configure the general query interval.
Use the **no** form of this command to restore the default value.
ip igmp query-interval *seconds*
no ip igmp query-interval

Parameter Description

Parameter	Description
seconds	General query interval. Its range is from 1 to 18000 in seconds.

Defaults

The general query interval is 125 seconds by default.

Command Mode

Interface configuration mode

Usage Guide

The interval of sending general query messages can be changed by configuration of general query interval .

Configuration Examples

The following example configures the general query interval to 120 seconds on interface Ethernet 0.

```
Ruijie(config-if)# ip igmp query-interval 120
```

The following example restores the general query interval to the default value on interface Ethernet 0.

```
Ruijie(config-if)# no ip igmp query-interval
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip igmp query-max-response-time

Use this command to configure the maximum response interval.
Use the **no** form of this command to set the maximum response interval to the default value.
ip igmp query-max-response-time *seconds*
no ip igmp query-max-response-time

Parameter Description

Parameter	Description
seconds	The maximum response interval. Its range is from 1 to 25 seconds.

Defaults The maximum response interval is 10 seconds by default.

Command Mode Interface configuration mode

Usage Guide Use this command to control the interval for the respondent to respond the query message before the device deletes the group information.

Configuration Examples

The following example configures the maximum response interval to 20 seconds on 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 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

ip igmp query-timeout

Use this command to configure the other querier present interval.

Use the **no** form of this command to restore the default value.

ip igmp query-timeout *seconds*

no ip igmp query-timeout

Parameter Description

Parameter	Description
seconds	Other querier present interval. Its range is from 60 to 300 seconds.

Defaults

The default time is 255 seconds.

Command Mode

Interface configuration mode

Usage Guide

By default, Cisco sets the waiting time of the device to twice of the query interval set by the **ip igmp query-interval** command. In Ruijie, the default value is set to 255 seconds. The device becomes the querier if no query packet is received within this duration.

Configuration Examples

The following example configures the other querier present interval to 200 seconds on interface Ethernet 0/1.

```
Ruijie(config-if)# ip igmp query-timeout 200
```

The following example restores the default value on interface Ethernet 0/1.

```
Ruijie(config-if)# no ip igmp query-timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

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 value.

ip igmp robustness-variable *number*

no ip igmp robustness-variable

Parameter Description

Parameter	Description
number	The value of robustness variable ranging from 2 to 7

Defaults

The default value 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 0/1
Ruijie(config-if)# ip igmp robustness-variable 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip igmp ssm-map enable

Use this command to enable the **igmp ssm-map** function in global configuration mode.

ip igmp [**vrf** *vrf-name*] **ssm-map enable**

no ip igmp [**vrf** *vrf-name*] **ssm-map enable**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies a VRF.

Defaults The **igmp ssm-map function** is disabled by default.

Command Mode Global configuration mode

Usage Guide If this command is run, 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 global configuration mode:

```
Ruijie(config)# ip igmp ssm-map enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

ip igmp ssm-map static

Use this command to map the static **ssm-map** source IP address to the group records in global configuration mode.

ip igmp [**vrf** *vrf-name*] **ssm-map static** *access-list a.b.c.d*

no ip igmp [**vrf** *vrf-name*] **ssm-map static** *access-list a.b.c.d*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies a VRF.
access-list	ACL in the range from 1 to 99, 1300 to 1999, or characters
a.b.c.d	Unicast address mapped to the group record

Defaults

No mapped source IP address is available 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 packets in versions earlier than **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

The **vrf** parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

ip igmp static-group

Use this command to directly add an interface of a device to a group.

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

ip igmp static-group *group-address*

no ip igmp static-group *group-address*

Parameter Description

Parameter	Description
group-address	IP address of the static group to which the interface is to be added

Defaults

The device is not added to any static group by default.

Command Mode Interface configuration mode

Usage Guide Use this command to directly add an interface of a device to a static group.

Configuration Examples

The following example adds interface Eth0/1 of a device to group 236.6.6.6.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ip igmp static-group 236.6.6.6
Ruijie(config-if)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 value.

ip igmp version { *1* | *2* | *3* }

no ip igmp version

Parameter Description

Parameter	Description
{ *1* | *2* | *3* }	Version number of IGMP ranging from 1 to 3

Defaults The version number is 2 by default.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the IGMP version. Note that IGMP will restart after configuration.

Configuration Examples

The following example sets the version number of IGMP to 2.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ip igmp version 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 [**vrf** *vrf-name*] **group** [*group-address* [*interface-type interface-number*]]

Parameter Description

Parameter	Description
N/A	Deletes all group information.
vrf *vrf-name*	Specifies a VRF.
group-address	32-bit multicast group IP address, namely Class-D address. 8 bits are in one group in decimal format. Groups are separated with dots.
interface-type	Type of the associated interface
interface-number	Number of the associated interface

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 the list. To delete all the entries from the IGMP buffer, run the **clear ip igmp group** command without specifying any parameters.

Configuration Examples The following example deletes all group entries from the IGMP buffer.

```
Ruijie# clear ip igmp group
```

Related Commands

Command	Description
show ip igmp groups	Displays all group member information.
show ip igmp interface	Displays interface information.

Platform Description The **vrf** parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

clear ip igmp interface

Use this command to clear the IGMP records for the interface.

clear ip igmp [**vrf** *vrf-name*] **interface** *ifname*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies a VRF.
ifname	Name of the interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the information generated when IGMP is configured on the interface.

Configuration Examples

```
Ruijie# clear ip igmp interface eth0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

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 [**vrf** *vrf-name*] **groups** [*interface-type interface-number*] [*group-address*] [**detail**]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies a VRF.
group-address	32-bit multicast group IP address, namely Class-D address. 8 bits are in one group in decimal format. Groups are separated with dots.
interface-type	Type of the associated interface
interface-number	Number of the associated interface
detail	Displays detailed information.
N/A	Displays information about all groups.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command without specifying any parameters to display the 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 specified in the command.

Configuration Examples

The following example displays information about all 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

The **vrf** parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

show ip igmp interface

Use this command to display the configuration of an interface.

show ip igmp [**vrf** *vrf-name*] **interface** [*interface-type interface-number*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies a VRF.
interface-type	Type of the associated interface
interface-number	Number of the associated interface
N/A	Displays information about all interfaces.

Defaults N/A

Command Mode Privileged EXEC mode

Configuration Examples

The following example displays the information of all interfaces.

```
Ruijie# show ip igmp interface
Interface vlan 1(Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds
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 The **vrf** parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

show ip igmp ssm-mapping

Use this command to display the ssm-map information of the IGMP configuration.

show ip igmp [**vrf** *vrf-name*] **ssm-mapping** [*A.B.C.D*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies a VRF.
A.B.C.D	Source address to be mapped

Defaults All ssm-map information of the IGMP is displayed by default.

Command Mode Privileged EXEC mode

Usage Guide If all parameters are not specified, the related configurations are displayed.

The following example displays the ssm-map configuration information.

```
Ruijie# sh ip igmp ssm-mapping
SSM Mapping: Enabled
Database  : Static mappings configured
```

Configuration Examples

The following example displays the group information to which group 233.3.3.3 is 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

The **vrf** parameter is supported only on RSR20, RSR30, RSR50, and RSR50E.

MLD Commands

clear ipv6 mld group

Use this command to clear the dynamic group member learned by MLD protocol.
clear ipv6 mld group [*group-address*] [*interface-type interface-number*]

Parameter Description

Parameter	Description
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

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. Those packet statistical information include the number of the received report packets, the number of the done packets and the the number of the group members on the interface.

Configuration Examples The following example clears all MLD statistical information and the group member records on the interface.

```
Ruijie# clear ipv6 mld interface fa 1/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld access-group

Use this command to filter the specific requested group on the interface. Only the report packets in accordance with the corresponding ACL are allowed to be processed.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld access-group *access-list*
no ipv6 mld access-group
default ipv6 mld access-group

Parameter Description

Parameter	Description
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.

The 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-Ethernet 0/1-Ethernet 0/1)# ipv6 mld access-group acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld immediate-leave group-list

Use this command to set the immediate-leave mechanism. With this command configured, the group within the range of group-list, will not send the query packet for the specific group and will remove this group from the group member list immediately after receiving the corresponding done packets. This function is used in the condition that there is only one multicast source that receives the host request on an interface. Use the **no** or **default** form of this command to restore the default setting.

ipv6 mld immediate-leave group-list *access-list*

no ipv6 mld immediate-leave group-list

default ipv6 mld immediate-leave group-list

Parameter Description

Parameter	Description
access-list	The IPv6 ACL name

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide

Without this command configured, when the device receives the MLD leave packets, the request packets for the specific groups will be sent. If there is still no host reply within the response time, the device will remove the corresponding group record from the group member list. The timeout interval is determined by the last member query interval and the MLD robustness variable, and the default value is 2 seconds.

With this command configured, when the device receives the MLD leave packets, it will not send the request packets for the specific groups, but remove the group information immediately, which reduces the leave delay greatly in the 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-Ethernet  0/1-Ethernet  0/1)#  ipv6  mld  immediate-leave
group-list acl
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld join-group

Use this command to configure the host action for the switch interface and add the related multicast group to the interface.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld join-group *group-address*
no ipv6 mld join-group *group-address*
default ipv6 mld join-group group-address

Parameter Description

Parameter	Description
group-address	The IPv6 non-management multicast group address, which cannot start with 0xFF*1, 0xFF*2, and 0xFF3*

Defaults The interface is not added to any group by default.

Command Mode Interface configuration mode

Usage Guide Use this command to enable the MLD host action on the interface. The interface can not only send the packets initiatively, but also reply to the query packets.
Use this command if it is necessary to join a group member to the interface.

Configuration Examples The following example adds the host group member:

```
=
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld join-group ff55::100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld last-member-query-count

Use this command to set the last-member-query-count number.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld last-member-query-count *number*
no ipv6 mld last-member-query-count
default ipv6 mld last-member-query-count

Parameter Description

Parameter	Description
number	The last member query count number. The valid range is 2 to 7.

Defaults The default is 2.

Command Mode Interface configuration mode

Usage Guide With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group (multiplied by the value of **mld last-member-query-count**) plus half the reply time.

Configuration 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-Ethernet 0/1)# ipv6 mld last-member-query-count 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld last-member-query-interval

Use this command to set the time interval of sending the query packets to the specific group.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld last-member-query-interval *interval*
no ipv6 mld ast-member-query-interval
default ipv6 mld last-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 seconds.

Command Mode Interface configuration mode

Usage Guide With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group(multiplied by the value of **mld last-member-query-count**) plus half the reply time.

Configuration Examples The following example sets the mld last-member-query-interval to 2 seconds.

```
Ruijie# configure terminal
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld last-member-query-interval 20
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

ipv6 mld limit

Use this command to enable to learn the max-number of the group member through the MLD protocol.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld limit *number* [**except** *access-list*]
no ipv6 mld limit *number* [**except** *access-list*]
default ipv6 mld limit ***number*** [**except** *access-list*]

Parameter Description

Parameter	Description
number	The maximum number of the group member learned by the MLD
except *access-list*	(Optional) The ACL beyond the configured mld limit

Defaults

Interface: 1,024
Global: 65,536

Command Mode

Interface configuration mode/Global configuration mode

Usage Guide

Use this command to set the max-number of the group members learned through the MLD in the global configuration mode. If the group member number has exceeded the limit, the received report packets later will be discarded and fail to form the group record.
If the except list has also been set at the same time, the group member packets, including the packets in the access-list, will be free from the member number limit.
This command can also be used in the interface configuration mode. The configurations in two different configuration modes are independent. If the number limit in the global configuration mode is lower than the one in the interface configuration mode, the former configuration takes precedence.

Configuration Examples

The following example sets the MLD limit to 400, but the configured ACL can still learn.

```
Ruijie(config-if)# ipv6 mld limit 300 except acl
Ruijie# configure terminal
Ruijie(config)# ipv6 mld limit 400 except acl1
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld limit 300 except acl1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 mld mroute-proxy

Use this command to enable the interface to forward the packets to the correspondent connected interface.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld mroute-proxy *interface-type interface-number*
no ipv6 mld mroute-proxy
default ipv6 mld mroute-proxy

Parameter 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 Use the **ipv6 mld proxy-service** command to configure the uplink interface as **proxy-service** one.
Use the **ipv6 mld mroute-proxy** command to configure the downlink interface as **mroute-proxy** one.
After the connected interface has been configured as the proxy-service interface, it can forward the MLD packets sent from other members.

Configuration Examples The following example sets the interface as the mroute-proxy interface and enables multicast proxy.

```
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld proxy-service
Ruijie(config-if-Ethernet 0/1)# exit
Ruijie(config)# interface eth 0/2
Ruijie(config-if-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld proxy-service

Use this command to enable the proxy-service function for the interface connected with the mroute-proxy interface in the downward direction. After configuring this command, the interface becomes the one connected with the mroute-proxy in the upward direction, and associates with and maintains the group information from the interfaces in the downward direction. Use the **no** or **default**

form of this command to disable the default setting.

ipv6 mld proxy-service

no ipv6 mld proxy-service

default ipv6 mld proxy-service

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide Use the **ipv6 mld proxy-service** command to configure the uplink interface as **proxy-service** one. Use the **ipv6 mld mroute-proxy** command to configure the downlink interface as **mroute-proxy** one. The configurable max-number limit is 32. The number of the interfaces with MLD Proxy enabled is limited by the number multicast interfaces supported device. After receiving the query packet, the proxy-service interface replies according to the member information, which are collected from the mroute-proxy interface and maintained by the proxy-service interface itself. With proxy-service configured, this interface owns the host action rather than the router action.

The **ipv6 mld mroute-proxy interface** command configuration on the associated interface in the downward direction is removed automatically if the switchport operation is performed on the interfaces.

Configuration Examples The following example sets the interface proxy-service and enables multicast proxy.

```
Ruijie(config)# interface eth 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld proxy-service
Ruijie(config-if-Ethernet 0/1)# exit
Ruijie(config)# interface eth 0/2
Ruijie(config-if-Ethernet 0/1-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld querier-timeout

Use this command to set the querier alive period.

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

ipv6 mld querier-timeout *seconds*

no ipv6 mld querier-timeout
default ipv6 mld querier-timeout

Parameter Description

Parameter	Description
seconds	The querier alive period, in the range from 60 to 300 in the unit of seconds.

Defaults The default is 255 seconds.

Command Mode Interface configuration mode

Usage Guide After the querier sends the query packet, the querier will wait to receive the query packet sent by another querier within the alive period. If no packet is received by the first querier within the alive period, then the first querier takes itself as the only querier on the network segment.

Configuration Examples The following example sets the querier alive period to 200 seconds.

```
Ruijie(config-if-Ethernet 0/1)# ipv6 mld querier-timeout 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld query-interval

Use this command to set the query interval for the general member.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld query-interval *seconds*
no ipv6 mld query-interval
default ipv6 mld query-interval

Parameter Description

Parameter	Description
seconds	The query interval for the general member, in the range from 1 to 18,000 in the unit of seconds.

Defaults The default is 125 seconds.

Command 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 0/1.

```
Ruijie(config-if-Ethernet 0/1)# ipv6 mld query-interval 120
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld query-max-response-time

Use this command to set the maximum response time.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld query-max-response-time *seconds*
no ipv6 mld query-max-response-time
default ipv6 mld query-max-response-time

Parameter Description

Parameter	Description
seconds	The maximum response time, in the range from 1 to 25 in the unit of seconds

Defaults The default is 10 seconds.

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 Ethernet 0/1.

```
Ruijie(config-if-Ethernet 0/1)# ipv6 mld query-max-response-time 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld robustness-variable

Use this command to set querier robustness value.

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

ipv6 mld robustness-variable *number*

no ipv6 mld robustness-variable

default ipv6 mld robustness-variable

Parameter Description

Parameter	Description
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 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld robustness-variable 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld ssm-map enable

Use this command to enable the mld ssm-map function.

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

ipv6 mld ssm-map enable

no ipv6 mld ssm-map enable

default ipv6 mld ssm-map enable

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide With this command configured, the group information dynamically learned will be added to the related source record forcibly. Usually, this command is set with the **ipv6 mld ssm-map static** command.

Configuration Examples The following example enables the mld ssm-map function in the global configuration mode.

```
Ruijie(config)# ipv6 mld ssm-map enable
Ruijie(config)# ipv6 mld ssm-map static 11 4444::1234
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld ssm-map static

Use this command to set the mld ssm-map static mapping source record in the global configuration mode.

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

ipv6 mld ssm-map static *access-list source-address*

no ipv6 mld ssm-map static *access-list source-address*

default ipv6 mld ssm-map static *access-list source-address*

Parameter Description

Parameter	Description
access-list	Sets the IPv6 ACL name.
source-address	Sets the unicast address for the group record mapping.

Defaults There is no mapping source address by default.

Command Mode Global configuration mode

Usage Guide This command is used with the **ipv6 mld ssm-map enable** command. With this command configured, the received mldv1 packets are mapped to the correspondent source record.

Configuration The following example maps all group record of the ACL name to the source address 4444::1234.

Examples

```
Ruijie(config)# ipv6 mld ssm-map enable
Ruijie(config)# ipv6 mld ssm-map static te 4444::1234
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld static-group

Use this command to add an interface to a group statically.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 mld static-group *group-address*
no ipv6 mld static-group *group-address*
default ipv6 mld static-group *group-address*

Parameter Description

Parameter	Description
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 ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ipv6 mld static-group ff55::3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld version

Use this command to set the MLD version number on the interface.

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

ipv6 mld version { **1** | **2** }

no ipv6 mld version

default ipv6 mld version

Parameter Description

Parameter	Description
{ **1** | **2** }	Sets the MLD version number.

Defaults The default is 2.

Command 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-Ethernet 0/1)# ipv6 mld version 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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

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 User EXEC mode/Privileged EXEC mode

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

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/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

PIM-DM Commands

ip pim dense-mode

Use this command to enable PIM-DM on the interface.

Use the **no** form of this command to disable the function.

ip pim dense-mode

no ip pim dense-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults PIM-DM is disabled by default.

Command Mode Interface configuration mode

Usage Guide

Caution

Before enabling the PIM-DM, enable the multicast forwarding function in global configuration mode. Otherwise, the multicast data packets cannot be forwarded even when the PIM-DM is enabled.

Once the PIM-DM is enabled, IGMP is enabled automatically on each interface.

During the execution of this command, if the system prompts "`Failed to enable PIM-DM on <Interface Name>, resource temporarily unavailable, please try again`", please re-configure this command.

During the execution of this command, if the system prompts "`PIM-DM Configure failed! VIF limit exceeded in NSM!!!`", it indicates that the number of configured multicast interfaces exceeds the upper limit. In this case, if it is still required to enable the PIM-DM on the interface, delete unnecessary PIM-DM, PIM-SM, or DVMRP interfaces.

It is not recommended to configure different IPv4multicast routing protocols on different interfaces of a device.

If the interface is of the tunnel type, note the following:

IPv4 multicasting is supported only on 4Over4 configuration tunnel, 4Over4 GRE tunnel, 4Over6 configuration tunnel, and 4Over6 GRE tunnel.

The multicasting function can also be enabled on tunnel interfaces that do not support multicasting, but no error message will be displayed, and no multicast packets will be received or sent.

Multicast tunnels can only be built on Ethernet interfaces. The nested tunnel and the multicast data QoS/ACL are not supported.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim dense-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip pim neighbor-filter

Use this command to enable neighbor filtering on the interface. If neighbor filtering is set, and a neighbor is denied by the filtering access list, PIM-DM will not establish the peering relationship with this neighbor or will terminate the established peering relationship with this neighbor.
Use the **no** form of this command to disable the neighbor filtering function.
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 of 1 to 99 and name ACL

Defaults Neighbor filtering is disabled on the interface by default.

Command Mode Interface configuration mode

Usage Guide 1) Only the neighbor address that meets the ACL filtering conditions can be used as the PIM neighbor of the current interface. The neighbor address that is denied by the ACL cannot be used as the PIM neighbor of the current interface.
2) Peering relationship refers to the interaction of protocol packets between 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.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim neighbor-filter 14
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 override-interval to the default value.

ip pim override-interval *interval-milliseconds*

no ip pim override-interval

Parameter Description

Parameter	Description
interval-milliseconds	In the range of 1 to 65535 milliseconds

Defaults The override-interval is 2500 milliseconds by default.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the override-interval (the pruning veto time) for the interface.

Configuration Examples The following example sets the override-interval to 3000 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

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 hello interval to the default value.

ip pim query-interval *interval-seconds*

no ip pim query-interval

Parameter Description

Parameter	Description
interval-seconds	In the range of 1 to 65535 seconds

Defaults The interval of sending the hello message is 30 seconds by default.

Command Mode Interface configuration mode

Usage Guide If the hello interval is set, the hello holdtime will be updated to 3.5 times of the hello interval.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim query-interval 123
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip pim propagation-delay

Use this command to reconfigure the propagation-delay of the hello message.

Use the **no** form of this command to restore the propagation-delay to the default value.

ip pim propagation-delay *interval-milliseconds*

no ip pim propagation-delay

Parameter Description

Parameter	Description
interval-milliseconds	In the range of 1 to 32767 milliseconds

Defaults The propagation-delay of the hello message is 500 milliseconds be default.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the propagation-delay (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

ip pim state-refresh disable

Use this command to prohibit the interface from processing and forwarding the PIM-DM state refresh messages.

Use the **no** form of this command to restore the PIM-DM state refresh function on the interface.

ip pim state-refresh disable

no ip pim state-refresh disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The state refresh messages are processed and forwarded by default.

Command Mode Global configuration mode

Usage Guide When the state refresh function is disabled, the PIM-DM state refresh messages are not processed and forwarded. The sent Hello message does not contain the state refresh option. The SR Cap field will not be processed when the Hello message is received.


Caution

It is not recommended to disable the state refresh function. This is because disabling this function may reconverge the PIM-DM multicast forwarding tree 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 messages.

```
Ruijie# configure terminal
Ruijie(config)# ip pim state-refresh disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 interval to the default value.
ip pim state-refresh origination-interval *interval-seconds*
no ip pim state-refresh origination-interval

Parameter Description

Parameter	Description
interval-seconds	In the range of 1 to 100 seconds

Defaults The interval of sending the PIM-DM state refresh message is 60 seconds by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ip pim state-refresh
origination-interval 65
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 Use this command to reconfigure the start time of the statistics and clear the PIM packet counter.

Configuration Examples

```
Ruijie# clear ip pim dense-mode track
```

Related Commands

Command	Description
show ip pim dense-mode track	Displays the statistics of the PIM packets.

Platform Description N/A

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 detailed information of the interface.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the information of 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
```

The fields in the output are described in the following table.

Field	Description
Address	Primary IP address of the PIM-DM interface
Interface	Name of the PIM-DM interface
VIF Index	VIF 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

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	Multicast group or source IP address
group-or-source-address	Multicast group or source IP address. The two addresses in this command cannot be the group IP address or source IP address at the same time.
summary	Displays the brief information of routing entries.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the 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

show ip pim dense-mode neighbor

Use this command to display the information about the PIM-DM neighbors.

show ip pim dense-mode neighbor [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the 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
```

The fields in the output are described in the following table.

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

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, or 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
```

The fields in the output are described in the following table.

Field	Description
Destination	Multicast source IP address
Nexthop Num	Number of next hops
Nexthop Addr	IP address of the 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

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, or interface configuration mode

Usage Guide Use this command to display the number of PIM packets sent and received since the beginning of the statistics. When the system starts up, it sets the start time of the statistics. Each time the **clear ip pim dense-mode track** command is invoked, the start time of the statistics is reconfigured and the PIM packet counter is cleared.

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

PIM-SM Commands

clear ip mroute

clear ip mroute [**vrf** *vrf-name*] {* | *group_address* [*source_address*] }

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
*	Deletes all the multicast routing entries.
group_address	Deletes the multicast routing entries of the specific group.
group_address source_address	Deletes the multicast routing entries of the specific group and source IP addresses.

Defaults Multicast routing entries are not deleted by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to delete multicast routing entries manually.

Configuration Examples

```
Ruijie# clear ip mroute *
Ruijie# clear ip mroute 224.2.2.2
Ruijie# clear ip mroute 224.2.2.2 2.2.2.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

clear ip mroute statistics

clear ip mroute [**vrf** *vrf-name*] **statistics** { * | *group_address* [*source_address*] }

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
*	Deletes the statistics of all multicast routing entries.
group_address	Deletes the statistics of the multicast routing entries of the specific group.

group_address source_address	Deletes the statistics of the multicast routing entries of the specific group and source IP addresses.

Defaults Statistics of multicast routing entries are not deleted by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to delete the statistics of multicast routing entries manually.

Configuration Examples

```
Ruijie# clear ip mroute statistics *
Ruijie# clear ip mroute statistics 224.2.2.2
Ruijie# clear ip mroute statistics 224.2.2.2 2.2.2.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

clear ip pim sparse-mode bsr rp-set

clear ip pim sparse-mode [**vrf** *vrf-name*] **bsr rp-set ***

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
*	Clears all RP-SET.

Defaults The RP-SET is not cleared by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to manually clear all the RP information learnt dynamically.

Configuration Examples

```
Ruijie# clear ip pim sparse-mode bsr rp-set *
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

clear ip pim sparse-mode track

clear ip pim sparse-mode [**vrf** *vrf-name*] **track**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults The start time of the statistics is not reconfigured and the PIM packet counter is not cleared by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to reconfigure the start time of the statistics and clear the PIM packet counter.

Configuration Examples

```
Ruijie# clear ip pim sparse-mode track
```

Related Commands

Command	Description
show ip pim sparse-mode track	Displays the statistics of PIM packets.

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip multicast-routing

ip multicast-routing [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults Multicast routing is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable multicast routing. To enable PIM-SM on an interface, you also need to run this command. Otherwise, PIM-SM is disabled even though the **ip pim sparse-mode** command

has been configured.

Configuration Examples

```
Ruijie(config)# ip multicast-routing
```

Related Commands

Command	Description
N/A	N/A

Platform Description

The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim accept-bsr list

ip pim [**vrf** *vrf-name*] **accept-bsr list** *accpet-bsr list*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
accpet-bsr list	The range is from 1 to 99, 1300 to 1999, or can be characters.

Defaults

The PIM-SM router receives all external BSM packets by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to limit the range of valid BSRs on the PIM-SM router.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim accept-bsr list 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim accept-crp list

ip pim [**vrf** *vrf-name*] **accept-crp list** *accpet-crp list*

Parameter Description

Parameter	Description

vrf *vrf-name*	Specifies the VRF.
accpet-crp list	The range is from 100 to 199, 2000 to 2699 or can be characters.

Defaults The elected BSR receives all external advertisements of candidate RPs by default.

Command Mode Global configuration mode

Usage Guide Configure this command on a candidate BSR. When this BSR becomes the elected BSR, it is able to limit the address range of the valid C-RP and the multicast group range it serves.

Configuration Examples

```
Ruijie (config)# comfigure terminal
Ruijie (config)# ip pim accept-crp list 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim accept-crp-with-null-group

ip pim [**vrf** *vrf-name*] **accept-crp-with-null-group**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

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 Configure this command on a 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 it considers that this C-RP supports all groups.

Configuration Examples

```
Ruijie (config)# configure terminal
Ruijie (config)# ip pim accept-crp-with-null-group
```

Related Commands

Command	Description

N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim accept-register list

ip pim [**vrf** *vrf-name*] **accept-register list** *access-lit*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
access-list	Access control list supporting numerical ACL in the range of 100 to 199 and 2000 to 2699 and name ACL

Defaults No restriction is imposed on the source and group IP addresses of register messages on RP by default.

Command Mode Global configuration mode

Usage Guide Use this command to restrict the source and group IP addresses of register messages on RP.

Configuration Examples

```
Ruijie (config)# ip pim accept-register list 100
Ruijie (config)# access-list 100 permit ip 192.168.195.0 0.0.0.255 225.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim bsr-candidate

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
interface-type interface-number	Specifies the interface.
hash-mask-length	(Optional) HASH mask length configured for electing the RP.

	Its range is from 0 to 32. The default value is 10.
priority-value	(Optional) Priority configured for the candidate BSR. Its range is from 0 to 255. The default value is 64.

Defaults The device is not a candidate BSR by default.

Command Mode Global configuration mode

Usage Guide A PIM-SM domain must contain a unique BootStrap Router (BSR). The BSR is responsible for collecting and issuing RP information. A unique recognized BSR is elected among multiple candidate BSRs based on the bootstrap packets. Before BSR information is available, candidate BSRs consider themselves to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. The bootstrap packets contain the address and priority of the BSR. Use this command to enable a device to send a bootstrap packet to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR information with the received bootstrap packet. If the received bootstrap packet is better, each neighbor saves the address in this bootstrap packet as the BSR address and forwards the .bootstrap information. Otherwise, they will discard this packet.
A candidate BSR considers itself to be the BSR until it receives a bootstrap message from another candidate BSR and is notified that this other candidate BSR has a higher priority value (or the same priority value, but with a higher IP address).

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim bsr-candidate gi 0/3 30 192
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim bsr-border

ip pim bsr-border

Parameter Description

Parameter	Description
N/A	N/A

Defaults This command is not configured by default. That is, the BSR border is not configured on the interface.

Command Mode Interface configuration mode

Usage Guide To avoid BSM flooding, use this command to configure BSR border on the interface. After the configuration, the interface discards 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 interface gi 0/3.

```
Ruijie# configure terminal
Ruijie(config)# interface gi 0/3
Ruijie(config-if)# ip pim bsr-border
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip pim dr-priority

ip pim dr-priority *priority-value*

Parameter Description

Parameter	Description
priority-value	The greater the value, the higher the priority is. The range is from 0 to 4294967294. The default value is 1.

Defaults The DR priority is 1 by default.

Command Mode Interface configuration mode

Usage Guide The following rules are applied in the selection a DR:
If the priority parameter of the Hello message is set for the devices in a LAN, the one with the highest priority is elected to be the DR. If several devices has the same priority, the one with the highest 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 with the highest IP address is elected to be the DR.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface gi 0/3
Ruijie(config-if)# ip pim dr-priority 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip pim ignore-rp-set-priority

ip pim [**vrf** *vrf-name*] **ignore-rp-set-priority**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults The RP priority of the RP-set is taken into account by default.

Command Mode Global configuration mode

Usage Guide Use this command to ignore the priority of the RP corresponding to the multicast group.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config-if)# ip pim ignore-rp-set-priority
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim jp-timer

ip pim [**vrf** *vrf-name*] **jp-timer** *interval-seconds*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
interval-seconds	In the range from 1 to 65535 seconds

Defaults The Join/Prune message is sent at the interval of 60 seconds by default.

Command Mode Global configuration mode

Usage Guide Use this command to set the interval of sending the Join/Prune message.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim jp-timer 50
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim mib

ip pim mib dense-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults The MIB of the sparse mode is used by default.

Command Mode Global configuration mode

Usage Guide Use this command when the MIB of the dense mode must be used.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config-if)# ip pim mib dense-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip pim neighbor-filter

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 Neighbor filtering 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. If a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or it will terminate the established peering relationship with this neighbor.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface gi 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	Configures the ACL.

Platform Description N/A

ip pim neighbor-tracking

ip pim neighbor-tracking

Parameter Description

Parameter	Description
N/A	N/A

Defaults Join constraint is enabled on the interface by default.

Command Mode Interface configuration mode

Usage Guide Use this command to disable join restraint on the interface. If join constraint is enabled, the interface is not allowed to send its Join message to the upstream neighbor when it receives a Join message that its neighbor sends to the upstream neighbor. Whereas, if join constrain is disabled, the interface is allowed to send its Join message to the upstream neighbor when it receives a Join message that its neighbor sends to the upstream neighbor. This enables upstream routers to track how many receivers in downstream based on all the received Join messages.

Configuration The following example disables join restraint on the interface.

Examples

```
Ruijie# configure terminal
Ruijie(config)# interface gi 0/3
Ruijie(config-if)# ip pim neighbor-tracking
```

Related Commands

Command	Description
ip pim propagation-delay	N/A

Platform Description N/A

ip pim override-interval

ip pim override-interface *interval-milliseconds*

Parameter Description

Parameter	Description
interval-milliseconds	In the range from 1 to 65535 milliseconds

Defaults The override interval of the Hello option is 2500 milliseconds by default.

Command Mode Interface configuration mode

Usage Guide Use this command to set the override interval for the interface.

Caution

Change of propagation delay or prune delay will affect the override interval of the Join/prune message. According to the protocol, the override interval of the Join/prune message must be less than its hold time; otherwise temporary interruption may occur. The override interval must be maintained and ensured by the network management.

Configuration Examples The following example sets the override interval to 3000 milliseconds.

```
Ruijie# configure terminal
Ruijie(config)# interface gi 0/3
Ruijie(config)# ip pim override-interval 3000
```

Related Commands

Command	Description
ip pim propagation-delay	Configures the propagation delay for the interface,

Platform Description N/A

ip pim propagation-delay

ip pim propagation-delay *interval-milliseconds*

Parameter Description

Parameter	Description
interval-milliseconds	In the range from 1 to 32765 milliseconds

Defaults The propagation delay of the Hello option is 500 milliseconds by default.

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 affect the override interval of the Join/prune message. According to the protocol, the override interval of the Join/prune message must be less than its hold time; otherwise temporary interruption may occur. The override interval must be maintained and ensured by the network management.

Configuration Examples The following example sets the propagation delay to 600 milliseconds.

```
Ruijie# configure terminal
Ruijie(config)# interface gi 0/3
Ruijie(config)# ip pim propagation-delay 600
```

Related Commands

Command	Description
ip pim override-interval	Configures the override interval for the interface.
Ip pim neighbor-tracking	Enables neighbor tracking on the interface.

Platform Description N/A

ip pim probe-interval

ip pim [**vrf** *vrf-name*] **probe**-**interface** *interval-seconds*

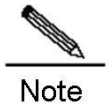
Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
interval-seconds	In the range from 1 to 65535 seconds

Defaults The register probe time is 5 seconds by default.

Command Mode Global configuration mode

Usage Guide Use this command to set the register probe time. The DR can send the null register message to the RP in a period before the register suppression time expires. This period is called probe time of null register packet.


Note

The probe time cannot be greater than half of the register suppression time. Otherwise, a warning will be displayed. In addition, the register suppression time times three and plus register probe time cannot be greater than 65535 seconds. Otherwise, a warning will also be displayed.

Configuration Examples The following example sets the register probe time to 6 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ip pim probe-interval 6
```

Related Commands

Command	Description
ip pim register-suppression	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim query-interval

ip pim query-interface *interval-seconds*

Parameter Description

Parameter	Description
interval-seconds	In the range from 1 to 65535 seconds

Defaults The Hello message is sent at the interval of 30 seconds by default.

Command Mode Interface configuration mode

Usage Guide Each time the interval of sending Hello messages is updated, the hold time of the Hello message will also be updated based on the following rule: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval multiplying 3.5 is greater than 65535 seconds, the transmission time will be forcibly updated to 18725 seconds.

Configuration

```
Ruijie# configure terminal
```

Examples

```
Ruijie(config)# interface gi 0/3
Ruijie(config)# ip pim query-interval 123
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip pim register-decapsulate-forward

ip pim [**vrf** *vrf-name*] **register-decapsulate-forward**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults By default, the RP does not decapsulate register packets or forward the multicast data packets contained in them.

Command Mode Global configuration mode

Usage Guide Use this command to enable a candidate RP to decapsulate the received PIM-SM register packets containing multicast data packets and forward the multicast data packets.

The decapsulation and forwarding are performed by the software. Therefore, it is not recommended to configure this command in the case that many register packets need to be decapsulated and forwarded; otherwise the CPU may be busy.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim register-decapsulate-forward
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim register-checksum-wholepkt

ip pim [**vrf** *vrf-name*] **register-checksum-wholepkt** [**group-list** *access-list*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
access-list	*access-list*: access control list supporting numerical ACL in the range from 1 to 99 and 1300 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 heads of PIM messages and register messages rather than the whole PIM messages.

Command Mode Global configuration mode

Usage Guide Devices of certain vendors calculate the checksum based on the whole PIM packets including the encapsulated multicast data packets. This command is introduced for the compatibility with these devices.

Configuration Examples

```
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	Configures the ACL.

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim register-rate-limit

ip pim [**vrf** *vrf-name*] **register-rate-limit** *rate*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
rate	Maximum number of register packets that can be sent per second, in the range from 1 to 65535

Defaults No rate limit is set for register messages by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the rate of transmitting register packets in (S, G) state rather than the rate of transmitting all register packets in the system. After this command is executed, the load of source DR and RP will be decreased. Only the register packets that do not exceed the rate limit can be transmitted.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim register-rate-limit 3000
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim register-rp-reachability

ip pim [**vrf** *vrf-name*] **register-rp-reachability**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults By default, the RP reachability is not checked before the transmission of register packets.

Command Mode Global configuration mode

Usage Guide Use this command to enable the function of checking the RP reachability before the transmission of register packets. If the RP is unreachable, register packets will not be transmitted.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim register-rp-reachability
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim register-source

ip pim [**vrf** *vrf-name*] **register-source** { *local_address* | *interface-type interface-number* }

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
local_address	Source IP address of register packets
interface-type interface-number	Interface whose IP address is used as the source IP address of register packets

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 Use this command to configure the source IP address of register packets.
The source IP address must be reachable. When the RP sends a correct Register-Stop message, the source IP address must be able to respond. It is recommended that the source IP address be the loopback IP address of the interface. Other physical IP addresses can also be used as the source IP address.

Caution It is not necessary to enable the PIM.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim register-source 192.168.195.80
Ruijie(config)# ip pim register-source gi 0/3
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim register-suppression

ip pim [**vrf** *vrf-name*] **register-suppression** *seconds*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

seconds	Suppression time in the range from 11 to 65535 seconds

Defaults The register packet suppression time is 60 seconds by default.

Command Mode Global configuration mode

Usage Guide Running this command on the DR will change the configured register packet suppression time. If the ip pim rp-register-kat command is not configured, running this command on the RP will change the period of RP keepalive.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim register-suppression 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim rp-address

ip pim [**vrf** *vrf-name*] **rp-address** *rp-address* [*access_list*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
rp-address	IP address of the RP
access_list	(Optional) Access control list supporting numerical ACL in the range from 1 to 99 and 1300 to 1999 and name ACL. All multicast groups are permitted 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 mechanism at the same time. When you use this command, note the following:

- 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 a static RP. But a static RP can be configured only once.
- If multiple static RPs serve a multicast group, the one with the highest IP address is

preferentially used.

- Only the addresses permitted by the ACL are valid multicast groups. All the multicast groups 224/4 are permitted by default.
- After the configuration is complete, the static RP's source IP address is inserted into 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 addresses. When an RP needs to be selected from a static RP group, the first entry, namely the one with the largest IP address, will be selected first.
- Deleting a static RP IP address will delete this address from all the existing static RP groups, and an address will be selected from the existing RP group tree structure as the RP address.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim rp-address 210.34.0.55 4
Ruijie(config)# access-list 4 permit 225.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	Configures the ACL.

Platform Description

The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim rp-candidate

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *access_list*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
interface-type interface-number	Interface
priority-value	(Optional) Priority in the range from 0 to 255. The default priority value is 192.
interval-seconds	(Optional) Interval in the range from 0 to 16383 seconds. The default interval is 60 seconds.
group_list *access_list*	(Optional) Numberical ACL in the range from 1 to 99 or name ACL. All multicast groups are permitted by default.

Defaults

No candidate RP is configured by default.

Command Mode

Global configuration mode

Usage Guide

According to the PIM-SM protocol, the shared tree RPT created by the multicast routing data uses the Rendezvous Point (RP) as the root node and group members as leaf nodes. RP is elected by the

candidate RPs. After BSR is elected, all C-RPs regularly send C-RP messages in the unicast form to the BSR, and the BSR spreads the messages throughout the PIM domain.
To specify an interface as the candidate RP of a specific group, run this command with ACL. Note that the group range is calculated only based on the permit ace, not the deny ace.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim rp-candidate gi 0/3 priority 200 group-list 3 interval 70
Ruijie(config)# access-list 3 permit 225.1.1.1 0.0.0.255
```

Related Commands

Command	Description
access-list	Configures the ACL.

Platform Description

The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim rp-register-kat

ip pim [**vrf** *vrf-name*] **rp-register-kat** *seconds*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
seconds	KAT timer time in the range from 1 to 65535 seconds

Defaults

The KAT timer length on the RP is 210 seconds by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the KAT interval of the RP.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# ip pim rp-register-kat 250
```

Related Commands

Command	Description
N/A	N/A

Platform Description

The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim sparse-mode

ip pim sparse-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults PIM-SM is disabled on the interface by default.

Command Mode Interface configuration mode

Usage Guide Use this command to enable PIM-SM on the interface.

Note

Enable multicast routing forwarding in global configuration mode before enabling PIM-SM. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM.

Once PIM-SM is enabled, the IGMP is enabled automatically on each interface.

During the execution of this command, if the messasge "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again" is displayed, re-execute this command.

During the execution of this command, if the message "PIM-SM Configure failed! VIF limit exceeded in NSM!!!" is displayed, it indicates that the number of configured interfaces exceeds the upper limit. Delete the unnecessary PIM-SM, PIM-DM, or DVMRP interfaces.

It is not recommended to configure different v4 multicast routing protocols on different interfaces of a device.

If the interface is of the tunnel type, note the following:

IPv4 multicasting is supported only on 4Over4 configuration tunnel, 4Over4 GRE tunnel, 4Over6 configuration tunnel, and 4Over6 GRE tunnel.

The multicasting function can also be enabled on tunnel interfaces that do not support multicasting, but no error message will be displayed, and no multicast packets will be received or sent.

Multicast tunnels can only be bulit on Ethernet interfaces. The nested tunnel and the multicast data QoS/ACL are not supported.

Configuration Examples

```
Ruijie# configure terminal
Ruijie(config)# interface gi 0/3
Ruijie(config-if)# ip pim sparse-mode
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

ip pim spt-threshold

ip pim [**vrf** *vrf-name*] **spt-threshold** [**group-list** *access_list*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
access_list	(Optional) Numerical ACL in the range from 1 to 99 and 1300 to 1999 or name ACL. By default, all multicast groups are permitted for SPT switching.

Defaults SPT switching is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the RP-to-SPT tree switching function in a specific multicast group range (specifying group-list) or all multicast groups (not specifying group-list).

Configuration Examples

```
Ruijie# configure terminal
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	Configures the ACL.

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim ssm

ip pim [**vrf** *vrf-name*] **ssm** {**default** | **range** *access_list*}

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
default	Multicast groups of 232/8

range *access_list*	Numerical ACL in the range from 1 to 99 or name ACL

Defaults PIM-SSM is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable PIM-SSM (or in specific multicast groups).

Configuration Examples The following example sets the source-specific multicast of the multicast group range 232/8.

```
Ruijie# configure terminal
Ruijie(config)# ip pim ssm default
The following example 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
access-list	Configures the ACL.

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

ip pim triggered-hello-delay

ip pim triggered-hello-delay *interval-seconds*

Parameter Description

Parameter	Description
interval-seconds	In the range from 1 to 5 seconds

Defaults The triggered-hello-delay is 5 seconds by default.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the triggered-hello-delay for the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and sends the Hello message within random time.

Configuration Examples The following example sets the triggered-hello-delay to 3 seconds.

```
Ruijie# configure terminal
Ruijie(config)# interface gi 0/3
Ruijie(config-if)# ip pim triggered-hello-delay 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show debugging

show debugging

Parameter Description

Parameter	Description
N/A	N/A

Defaults The status of the debugging switch is not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display the status of the debugging switch.

Configuration Examples The following example displays the status of the debugging switch.

```
Ruijie # show debugging
PIM-SM Debugging status:
PIM packet debugging is on.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip pim sparse-mode bsr-router

show ip pim sparse-mode [**vrf** *vrf-name*] **bsr-router**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults The BSR information is not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command 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 The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode interface

show ip pim sparse-mode [**vrf** *vrf-name*] **interface** [*interface-type interface-number* [**detail**]]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
interface-type interface-number	(Optional) Specifies the Interface. This command takes effect for all interfaces by default.
detail	(Optional) Displays detailed information of an interface.

Defaults The PIM-SM information on the interface is not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display 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 3):
  Address 30.30.100.200, DR 30.30.100.200
  Hello period 30 seconds, Next Hello in 11 seconds
  Triggered Hello period 5 seconds
  Neighbors:
   2.2.2.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode local-members

show ip pim sparse-mode [**vrf** *vrf-name*] **local-member** [*interface-type interface-number*]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
interface-type interface-number	(Optional) Specifies the interface. This command takes effect for all interfaces by default.

Defaults The local IGMP information on the PIM-SM-enabled interface is not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display the local IGMP information on the PIM-SM-enabled interface.

Configuration Examples The following example displays the local IGMP information on the PIM-SM-enabled 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 The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode mroute

show ip pim sparse-mode [**vrf** *vrf-name*] **mroute** [*group-or-source-address* [*group-or-source-address*]] [**proxy**]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
group-or-source-address	Group or source IP address
group-or-source-address	Group or source IP address. The two addresses in this command cannot be the group IP address or source IP address at the same time.
proxy	Displays the RPF Vector information carried by the entry.

Defaults Multicast routing entries are not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display routing information. Only one group IP address, one source IP address, or one group IP address-source IP address pair can be specified at a time. You can also specify no group IP address or source IP address.

Configuration Examples The following example displays routing information.

```
Ruijie#show ip pim sparse-mode mroute
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** and proxy parameters are supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode neighbor

show ip pim sparse-mode [**vrf** *vrf-name*] **neighbor** [**detail**]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
detail	(Optional) Displays detailed information of an interface.

Defaults Neighbor information is not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display the information of neighbors.

Configuration Examples The following example displays the information of neighbors

```
Ruijie#show ip pim sparse-mode neighbor
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode nexthop

show ip pim sparse-mode [**vrf** *vrf-name*] **nexthop**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults The information of the next hop is not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display the information of the next hop, including interface ID, IP address, and metric.

Configuration Examples

```
Ruijie# show ip pim sparse-mode nexthop
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode rp mapping

show ip pim sparse-mode [**vrf** *vrf-name*] **rp mapping**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults RPs and the multicast groups they serve are not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display the information of all RPs and the multicast groups they serve.

Configuration Examples The following example displays the information of 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 The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode rp-hash

show ip pim sparse-mode [**vrf** *vrf-name*] **rp-hash** *group-address*

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.
group-address	Group address to be resolved

Defaults The information of the RP of the specific group IP address is not displayed by default.

Command Privileged EXEC mode, global configuration mode, or interface configuration mode

Mode

Usage Guide Use this command to display the information of the RP of the specific group IP address.

Configuration Examples The following example displays the information of the RP of the specific group IP address.

```
Ruijie# show ip pim sparse-mode rp-hash 225.1.1.1
RP: 30.30.100.1
Info source: 30.30.100.1, via bootstrap
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

show ip pim sparse-mode track

show ip pim sparse-mode [**vrf** *vrf-name*] **track**

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF.

Defaults The statistics of PIM packets are not displayed by default.

Command Mode Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide Use this command to display the number of PIM packets sent and received since the beginning of the statistics. When the system starts up, it sets the start time of the statistics. Each time the **clear ip pim sparse-mode track** command is invoked, the start time of the statistics is reconfigured and the PIM packet counter is cleared.

Configuration Examples The following example displays the statistics of PIM packets.

```
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

The **vrf** parameter is supported only on the RSR20, RSR30, RSR50, and RSR50E.

PIM-SMv6 Commands

clear ipv6 mroute

Use this command to clear multicast routing entries.

clear ipv6 mroute {* | *ipv6_group_address* [*ipv6_source_address*] }

Parameter Description

Parameter	Description
*	Deletes all the multicast routing entries.
ipv6_group_address	Deletes the multicast routing entries of the specific group.
ipv6_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 N/A

Configuration Examples The following example clears all the multicast routing entries.

```
Ruijie# clear ipv6 mroute *
```

The following example clears the multicast routing entries of the specified group.

```
Ruijie# clear ipv6 mroute ff66::6666
```

The following example clears the multicast routing entries of the specified group and source address.

```
Ruijie# clear ipv6 mroute ff66::6666 3333::3333
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear ipv6 mroute statistics

Use this command to delete the statistics of the multicast routing entries.

clear ipv6 mroute statistics {* | *ipv6_group_address* [*ipv6_source_address*] }

Parameter

Parameter	Description

Description

*	Deletes the statistics of all multicast routing entries.
ipv6_group_address	Deletes the statistics of the multicast routing entries of the specific group.
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 N/A

Configuration Examples The following example deletes the statistics of the multicast routing entries.

```
Ruijie# clear ipv6 mroute statistics *
```

The following example clears the statistics of the multicast routing entries of the specified group.

```
Ruijie# clear ipv6 mroute statistics ff66::6666
```

The following example clears the statistics of the multicast routing entries of the specified group and source address.

```
Ruijie# clear ipv6 mroute statistics ff66::6666 3333::3333
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Only the RP information learnt dynamically can be cleared manually.

Configuration Examples The following example clears the RP information learnt dynamically.

```
Ruijie# clear ipv6 pim sparse-mode bsr rp-set *
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear ipv6 pim sparse-mode track

Use this command to reconfigure the start time of the statistics and clear the PIMv6 packet counter.

clear ipv6 pim sparse-mode track

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration 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

ipv6 multicast-routing

ipv6 multicast-routing

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Global configuration mode

Usage Guide This command is mandatory for enabling multicast routing and enabling PIM-SMv6 on an interface. Otherwise, PIM-SMv6 is disabled even though the ipv6 pim sparse-mode command is configured.

Configuration Examples

```
Ruijie(config)# ipv6 multicast-routing
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim accept-bsr list

Use this command to confine the BSR address range.

Use the **no** or **default** form this command to restore the default setting.

ipv6 pim accept-bsrr list *ipv6_access-list*

no ipv6 pim accept-bsr

default ipv6 pim accept-bsr

Parameter Description

Parameter	Description
list *ipv6_access-list*	IPv6 ACL supporting named ACL

Defaults By default, the PIM-SMv6 router receives all external BSM packets.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example confines the BSR address range.

```
Ruijie(config)# ipv6 pim accept-bsr list bsr-list
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim accept-crp-with-null-group

Use this command to receive the C-RP-ADV packets whose prefix-count is 0.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim accept-crp-with-null-group
no ipv6 pim accept-crp-with-null-group
default ipv6 pim accept-crp

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.

Configuration Examples The following example receives the C-RP-ADV packets whose prefix-count is 0.

```
Ruijie (config)# ipv6 pim accept-crp-with-null-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim accept-crp list

Use this command to confine the C-RP address range and the multicast group address range it serves.
Use the **no** or **default** form of this command to restore the default setting,
i**pv6 pim accept-crp list** *ipv6_access-list*
no ipv6 pim accept-crp
default ipv6 pim accept-crp-with-null-group

Parameter Description

Parameter	Description
list *ipv6_access-list*	IPv6 ACL supporting named 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)# ipv6 pim accept-crp list crp-list
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim accept-register

Use this command to accept specific register packets at the RP.

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

ipv6 pim accept-register { **list** *ipv6_access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *ipv6_access-list*] }

no ipv6 pim accept-register

default ipv6 pim accept-register

Parameter Description

Parameter	Description
list *ipv6_access-list*	IPv6 ACL supporting named ACL
route-map *map-name*	Defines the routing map rule

Defaults All register packets are received 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 denies register packets of the specified source address at the RP.

```
Ruijie(config)# ipv6 pim accept-register list register-access-list
Ruijie(config)# ipv6 access-list register-access-list
Ruijie(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
```

Platform Description N/A

ipv6 pim bsr-border

Use this command to configure the BSR border.

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

ipv6 pim bsr-border

no ipv6 pim bsr-border

default ipv6 pim bsr-border

Parameter Description

Parameter	Description
N/A	N/A

Defaults No BSR border is configured by default.

Command 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 *gi 0/3*.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet)# ipv6 pim bsr-border
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim bsr-candidate

Use this command to configure the candidate bootstrap router (C-BSR).

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

ipv6 pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]
no ipv6 pim bsr-candidate
default ipv6 pim bsr-candidate

Parameter Description

Parameter	Description
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 C-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(config)# ipv6 pim bsr-candidate gi 0/3 30 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim dr-priority

Use this command to configure the DR priority.

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

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority

default ipv6 pim dr-priority

Parameter Description

Parameter	Description
priority-value	The larger the value, the higher the priority is. The range is from 0 to 4,294,967,294. The default is 1.

Defaults The default is 1.

Command Mode Interface configuration mode

Usage Guide To select a DR:

- If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices have the same priority, the one of the largest IP address is elected to be the DR.
- If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.

Configuration Examples The following example configures the DR priority.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if)# ipv6 pim dr-priority 11234
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim ignore-rp-set-priority

Use this command to ignore the RP priority.

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

ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority

default ipv6 pim ignore-rp-set-priority

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the C-RP with a higher priority is selected.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example ignores the RP priority.

```
Ruijie(config-if)# ipv6 pim ignore-rp-set-priority
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim jp-timer

Use this command to set the interval to send the join/prune message.

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

ipv6 pim jp-timer *seconds*

no ipv6 pim jp-timer

default ipv6 pim jp-timer

Parameter Description

Parameter	Description
seconds	Interval to send the join/prune message in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide This command is used to set the interval to send the Join/Prune message.

Configuration Examples The following example sets the interval to send the Join/Prune message to 100 seconds.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 pim jp-timer 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim neighbor-filter

Use this command to confine the neighbor address range.

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

ipv6 pim neighbor-filter *ipv6_access-list*

no ipv6 pim neighbor-filter *ipv6_access-list*

default ipv6 pim neighbor-filter *ipv6_access-list*

Parameter Description

Parameter	Description
ipv6_access_list	IPv6 ACL supporting named ACL

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.

Configuration Examples The following example blocks the neighbor address fe80::2d0:f8ff:fe22:33ad.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if- GigabitEthernet 0/3)# ipv6 pim neighbor-filter acl
Ruijie(config-if- GigabitEthernet 0/3)# exit
Ruijie(config)# ipv6 access-list acl
Ruijie(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any
```

Related Commands

Command	Description
ipv6_access-list	N/A

Platform Description N/A

ipv6 pim neighbor-tracking

Use this command to disable join restraint on the interface.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim neighbor-tracking
no ipv6 pim neighbor-tracking
default ipv6 pim neighbor-tracking

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.

Configuration Examples The following example disables join restraint on the interface.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet)# ipv6 pim neighbor-tracking
```

Related Commands

Command	Description
ipv6 pim propagation-delay	N/A

Platform Description N/A

ipv6 pim override-interval

Use this command to set the override-interval on the interface.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim override-interval *milliseconds*
no ipv6 pim override-interval
default ipv6 pim override-interval

Parameter

Parameter	Description

Description

milliseconds	In the range 1 to 65,535 in the unit of milliseconds

Defaults The default is 2,500 milliseconds.

Command Mode Interface configuration mode

Usage Guide Use this command to set the override-interval for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration Examples The following example sets the override-interval to 3,000 milliseconds.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet)# ipv6 pim override-interval 3000
```

Related Commands

Command	Description
ipv6 pim propagation-delay	N/A

Platform Description N/A

ipv6 pim probe-interval

Use this command to set the register probe interval.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim probe-interval *seconds*
no ipv6 pim probe-interval
default ipv6 pim probe-interval

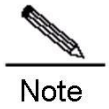
Parameter Description

Parameter	Description
seconds	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 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(config)# ipv6 pim probe-interval 6
```

Related Commands

Command	Description
ipv6 pim register-suppression	N/A

Platform Description N/A

ipv6 pim propagation-delay

Use this command to set the propagation-delay on the interface.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim propagation-delay *milliseconds*
no ipv6 pim propagation-delay
default ipv6 pim propagation-delay

Parameter Description

Parameter	Description
milliseconds	In the range from 1 to 32,765 in the unit of milliseconds

Defaults The default is 500 milliseconds.

Command Mode Interface configuration mode

Usage Guide Use this command to set the propagation-delay for the interface.

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration Examples The following example sets the propagation delay to 600 milliseconds.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim propagation-delay 600
```

Related Commands

Command	Description
ipv6 pim override-interval	N/A
ipv6 pim neighbor-tracking	N/A

Platform Description N/A

ipv6 pim query-interval

Use this command to set the interval to send the hellp packets.

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

ipv6 pim query-interval *seconds*

no ipv6 pim query-interval

default ipv6 pim query-interval

Parameter Description

Parameter	Description
seconds	Interval to send the Hello message in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 30.

Command Mode Interface configuration mode

Usage Guide Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18725.

Configuration Examples The following example sets the interval to send the hello packets.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim query-interval 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim register-checksum-wholepkt

Use this command to calculate the checksum of the whole register packet.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim register-checksum-wholepkt [**group-list** *ipv6_access-list*]
no ipv6 pim register-checksum-wholepkt [**group-list** *ipv6_access-list*]
default ipv6 pim register-checksum-wholepkt [**group-list** *ipv6_access-list*]

Parameter Description

Parameter	Description
group-list *ipv6_access-list*	IPv6 ACL supporting named ACL. *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(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

ipv6 pim register-rate-limit

Use this command to limit the rate of register packets.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim register-rate-limit *rate*
no ipv6 pim register-rate-limit
default ipv6 pim register-rate-limit

Parameter

Parameter	Description

Description

rate	Maximum number of register packets that can be sent per second, in the range from 1 to 65,535.

Defaults By default, there is no rate limitation on register messages.

Command Mode Global configuration mode

Usage Guide This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.

Configuration Examples The following example limits the rate of register packets.

```
Ruijie(config)# ipv6 pim register-rate-limit 3000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim register-rp-reachability

Use this command to check RP reachability before sending register packets**.**
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim register-rp-reachability
no ipv6 pim register-rp-reachability
default ipv6 pim register-rp-reachability

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the RP reachability is not checked before sending register packets.

Command Mode Global configuration mode

Usage Guide This command is used to check the RP reachability before transmission. If not, register packets are not transmitted.

Configuration The following example checks the RP reachability before sending register packets.

Examples

```
Ruijie(config)# ipv6 pim register-rp-reachability
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim register-source

Use this command to specify the source IPv6 address in the register packets.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim register-source { *ipv6_local_address* | *interface-type interface-number* }
no ipv6 pim register-source
default ipv6 pim register-source

Parameter Description

Parameter	Description
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.


Caution 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(config)# ipv6 pim register-source 3333::3333
Ruijie(config)# ipv6 pim register-source gi 0/3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim register-suppression

Use this command to set the register suppression time.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim register-suppression *seconds*
no ipv6 pim register-suppression
default ipv6 pim register-suppression

Parameter Description

Parameter	Description
seconds	Suppression time in the range from 1 to 65,535 in the unit of seconds

Defaults The default is 60 seconds.

Command Mode Global configuration mode

Usage Guide Executing this command on the DR will change the register packet suppression time configured. if the ipv6 pim rp-register-kat command is not configured, executing this command on RP will modify the period of RP keepalive.

Configuration Examples The following example sets the register packet suppression time.

```
Ruijie(config)# ipv6 pim register-suppression 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim rp-address

Use this command to configure the static RP.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access_list*]
no ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access-list*]
default ipv6 pim rp-address *ipv6_rp-address* [*ipv6_access-list*]

Parameter

Parameter	Description

Description

ipv6_rp-address	IPv6 address of RP
ipv6_access_list	IPv6 ACL supporting named 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(config)# ipv6 pim rp-address 3333::3333 acl
Ruijie(config)# ipv6 access-list acl
Ruijie(config)# permit ipv6 any ff66::6666/64
```

Related Commands

Command	Description
ipv6 access-list	N/A

Platform Description N/A

ipv6 pim rp-candidate

Use this command to configure the candidate RP (C-RP).

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

ipv6 pim rp-candidate *interface-type interface-number* [**priority** *priority-value*] [**interval**

interval-seconds] [**group-list** *ipv6_access-list*]

no ipv6 pim rp-candidate [*interface-type interface-number*]

default ipv6 pim rp-candidate [*interface-type interface-number*]

Parameter Description

Parameter	Description
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) IPv6 ACL supporting named ACL

Defaults N/A

Command Mode Global configuration mode

Usage Guide In the PIM-SMv6 protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain.

To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.

Configuration Examples The following example configures the RP candidate.

```
Ruijie(config)# ipv6 pim rp-candidate gi 0/3 priority 200 group-list acl interval 40
Ruijie(config)# ipv6 access-list acl
Ruijie(config-ipv6-acl)# permit ipv6  any ff66::6666/64
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim rp-register-kat

Use this command to set the Keepalive Timer (KAT) of a (S, G) entry created by the register packet at the RP.

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

ipv6 pim rp-register-kat *seconds*

no ipv6 pim rp-register-kat

default ipv6 pim rp-register-kat

Parameter Description

Parameter	Description
seconds	KAT value in the range from1 to 65,525 in the unit of seconds.

Defaults The default is equal to the sum of register probe time and three times register suppression time.

Command Mode Global configuration mode

Usage Guide The KAT value at the RP should be greater than three times the register suppression time at the source DR. Otherwise, the KAT will end and the entry (S,G) will time out before another register packet is sent, so that multicast stream will break down in a short while.

Configuration Examples The following example configures the KAT interval of RP.

```
Ruijie(config)# ipv6 pim rp-register-kat 250
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim rp embedded

Use this command to enable the embedded RP function.

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

ipv6 pim rp embedded [**group-list** *ipv6_acl_name*]

no ipv6 pim rp embedded

default ipv6 pim rp embedded

Parameter Description

Parameter	Description
group-list *ipv6_acl_name*	IPv6 ACL

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the embedded RP function explicitly and to enable the embedded

RP for the IPv6 multicast address of specified embedded RP address.

Configuration Examples The following example enables the embedded RP for the IPv6 multicast addresses of all embedded RP addresses.

```
Ruijie(config)# ipv6 pim rp embedded
```

Related Commands

Command	Description
ipv6 access-list	N/A

Platform Description N/A

ipv6 pim sparse-mode

Use this command to enable PIM-SMv6 on the interface.

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

ipv6 pim sparse-mode

no ipv6 pim sparse-mode

default ipv6 pim sparse-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to enable PIM-SMv6 on the interface.

Note 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.

Note 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.

Note 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.


Note

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.


Note

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(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim sparse-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim spt-threshold

Use this command to enable SPT switch.

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

ipv6 pim spt-threshold [**group-list** *ipv6_access-list*]

no ipv6 pim spt-threshold [**group-list** *ipv6_access-list*]

default ipv6 pim spt-threshold [**group-list** *ipv6_access-list*]

Parameter Description

Parameter	Description
ipv6_access_list	(Optional) IPv6 ACL supporting named ACL

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast

group range (using group-list) or all multicast groups (not using group-list) .

Configuration 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

ipv6 pim ssm

Use this command to enable SSM and set the SSM group address range.

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

ipv6 pim ssm { **default** | **range** *ipv6_access-list* }

no ipv6 pim ssm

default ipv6 pim ssm

Parameter Description

Parameter	Description
default	Group in the range of FF3x::/32
range *ipv6_access_list*	IPv6 ACL supporting named ACL

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to enable 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 aclRuijie(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

ipv6 pim static-rp-preferred

Use this command to configure a higher priority for static RP over the C-RP.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim static-rp-preferred
no ipv6 pim static-rp-preferred
default ipv6 pim static-rp-preferred

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the priority of the RP elected through BSR mechanism is high than the one configured statically.

Command 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(config-if)# ipv6 pim static-rp-preferred
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 pim triggered-hello-delay

Use this command to configure Triggered-Hello-Delay time on the interface.
Use the **no** or **default** form of this command to restore the default setting.
ipv6 pim triggered-hello-delay *seconds*
no ipv6 pim triggered-hello-delay
default ipv6 pim triggered-hello-delay

Parameter

Parameter	Description

Description

seconds	In the range from1 to 5 in the unit of seconds.

Defaults The default is 5 seconds.

Command Mode Interface configuration mode

Usage Guide Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message at the random time.

Configuration Examples The following example sets the triggered-hello-delay to 3 seconds.

```
Ruijie(config)# interface gi 0/3
Ruijie(config-if-GigabitEthernet 0/3)# ipv6 pim triggered-hello-delay 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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 N/A

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

show ipv6 pim sparse-mode bsr-router

Use this command to display the BSR information.

show ipv6 pim sparse-mode bsr-router

Parameter Description

Parameter	Description
N/A	N/A

Defaults Privileged EXEC mode/Global configuration mode /Interface configuration mode

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

Usage Guide N/A

Configuration 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

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 N/A

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

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 N/A

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

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

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

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	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 N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 pim sparse-mode rp mapping

Use this command to display the information on all RPs and the multicast groups they serve.

show ipv6 pim sparse-mode rp mapping

Parameter Description

Parameter	Description
mapping	All groups and RP information.

Defaults N/A

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

Usage Guide N/A

Configuration 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

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 N/A

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

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

Ruijie Multicast Express Forward Commands

ip ref

Use this command to enable Ruijie multicast express forward (RMEF) on the specifed interface. Use the **no** form of this command to disable the function.

ip ref

no ip ref

Parameter Description

Parameter	Description
N/A	N/A

Defaults RMEF is enabled on the interface by default.

Command Mode Interface configuration mode

Usage Guide Use this command to enable RMEF (including the multicast express forwarding) on an interface.

Configuration Examples The following example enables RMEF on interface fastEthernet 0/0.

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if)# ip ref
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip ref mcast route

Use this command to display information of RMEF.

show ip ref mcast route [*source-address group-address*]

Parameter Description

Parameter	Description
source-address group-address	Displays information of RMEF based on the source IP address and multicast group address.
N/A	Displays information of all RMEFs.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide Use this command to display information of RMEF.

Configuration Examples

The following example displays information of RMEF.

```
Ruijie# show ip ref mcast route 30.1.1.2, 224.1.1.2
IP Multicast EF Routing Table
Interface State: Interface (Interface Index)
(30.1.1.2, 224.1.1.2)
 In_interface: GigabitEthernet 0/1.100(8)
 Hit: Yes
 To_cpu: No
 Oif_list: GigabitEthernet 0/2.100(12)

Ruijie# show ip ref mcast route
IP Multicast EF Routing Table
Interface State: Interface (Interface Index)
(30.1.1.2, 224.1.1.2)
 In_interface: GigabitEthernet 0/1.100(8)
 Hit: Yes
 To_cpu: No
 Oif_list: GigabitEthernet 0/2.100(12)
Ruijie# show ip ref mcast route 60.1.1.3, 238.1.1.1
(60.1.1.3, 238.1.1.1)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip ref mcast info

Use this command to display statistics and rate limit of RMEF.

show ip ref mcast info

Parameter Description

Parameter	Description
N/A	Statistics and rate limit of RMEF.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display statistics and rate limit of RMEF. Based on the statistics, you can know the working conditions of RMEF.

Configuration Examples The following example displays statistics and rate limit of RMEF.

```
Ruijie# show ip ref mcast info
--------------------------------
IP RMEF is open
total RMEF MFC NUM = 1
to_cpu ratelimit PPS in one second = 10
no_mfc ratelimit PPS in one second = 10
--------------------------------
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip ref mcast statistics

Use this command to display statistics of forwarded packets of RMEF.

show ip ref mcast statistics { **interface** *interface-type interface-number* | **mfc** }

Parameter Description

Parameter	Description
Interface *interface-type interface-number*	Displays statistics of forwarded packets of RMEF on the specified interface.
mfc	Displays statistics of forwarded packets all RMEF forwarding entries.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display statistics of forwarded packets of RMEF.

Configuration Examples The following example displays statistics of forwarded packets of RMEF.

```
Ruijie# show ip ref mcast mfc interface GigabitEthernet 0/1.100
(30.1.1.2, 224.1.1.2)
 In_interface: GigabitEthernet 0/1.100(8)
```

```
 Match_PKTNUM: 17058555
 Match_PKTBYTES: 1091747520
 WRONG_IN_IF_PKTNUM: 0
 TO_CPU_RESERVE_PACKET: 0
 TO_CPU_DROP_PACKET: 0
 Oif_list: GigabitEthernet 0/2.100(12)


Ruijie# show ip ref mcast mfc
(30.1.1.2, 224.1.1.2)
 In_interface: GigabitEthernet 0/1.100(8)
 Match_PKTNUM: 17058555
 Match_PKTBYTES: 1091747520
 WRONG_IN_IF_PKTNUM: 0
 TO_CPU_RESERVE_PACKET: 0
 TO_CPU_DROP_PACKET: 0
 Oif_list: GigabitEthernet 0/2.100(12)
(40.1.1.2, 224.1.1.4)
 In_interface: GigabitEthernet 0/1.200(9)
 Match_PKTNUM: 170585333
 Match_PKTBYTES: 109174567
 WRONG_IN_IF_PKTNUM: 0
 TO_CPU_RESERVE_PACKET: 0
 TO_CPU_DROP_PACKET: 0
 Oif_list: GigabitEthernet 0/2.400(14)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

MSDP Commands

clear ip msdp peer

Use this command to clear specific MSDP peer. This will clear the connection to the MSDP peer and then reestablish the connection to MDSP peer. The statistics of MSDP peer will be cleared at the same time.

clear ip msdp peer *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear the TCP connection to the specified MSDP peer and clear all the MSDP peer statistics.

Configuration Examples The following example clears MDSP peer of 218.14.5.23.

```
Ruijie# clear ip msdp peer 218.14.5.23
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

clear ip msdp sa-cache

Use this command to clear SA cache entries.

clear ip msdp sa-cache [*group-address*]

Parameter Description

Parameter	Description
group-address	Group address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the SA cache entries learned from MSDP peer. If no multicast group address is specified, all SA cache entries will be cleared.
After SA cache entries are cleared, the MSDP device will need to relearn SA messages.

Configuration Examples The following example clears the SA cache entries with the multicast group 224.1.1.1.

```
Ruijie# clear ip msdp sa-cache 224.1.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

clear ip msdp statistics

Use this command to clear the statistics of MSDP peers without resetting the TCP sessions.
clear ip msdp statistics [*peer-address*]

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer whose statistics counters, reset count, and input/output count will be cleared.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear the statistics of MSDP peers and view the new statistics of MSDP peers. This command can clear the statistics of one or more MDSP peers without resetting the MSDP peer.

Configuration Examples The following example clears the statistics of the MSDP peer with IP address being 61.83.1.52.

```
Ruijie# clear ip msdp statistics 61.83.1.52
```

Related Commands

Command	Description
N/A	N/A

Platform This command is supported only on L3 devices.

Description

ip msdp default-peer

Use this command to define a default MSDP peer.
Use **no** or **default** form of this command to restore the default setting.
ip msdp default-peer *peer-address* [**prefix-list** *prefix-list-name*]
no ip msdp default-peer *peer-address*
default ip msdp default-peer *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer
prefix-list *prefix-list-name*	Specifies the BGP prefix list.

Defaults By default, no default MSDP peer is configured.

Command Mode Global configuration mode

Usage Guide The RPF-Peer calculation rule for the specified RP address may leads the loss of RPF-Peer information, which causes that the SA messages are dropped directly without the Peer-RPF check. With a default peer configured, the SA messages are ensured to pass the Peer-RFP check, so that the local host could accept the SA messages to learn the multicast source information carried by the SA messages.
If "prefix-list prefix-list-name" is not specified, all SA messages from the default MSDP peer will be accepted.
If "prefix-list prefix-list-name" is specified, only the SA messages from the RP specified by prefix-list prefix-list-name will be accepted.
If "prefix-list prefix-list-name" is specified but the prefix list is not configured, all SA messages from this default MSDP peer will be accepted.

Configuration Examples The following example configures 172.16.33.1 as the default peer.

```
Ruijie(config)# ip msdp peer 172.16.33.1
Ruijie(config)# ip msdp peer 172.16.34.2
Ruijie(config)# ip msdp default-peer 172.16.33.1
```

Related Commands

Command	Description
ip msdp peer	Creates MSDP peer.

Platform Description This command is supported only on layer-3 device.

ip msdp description

Use this command to add descriptive information for MSDP peer.
Use **no** or **default** form of this command to restore the default setting.
ip msdp description *peer-address text*
no ip msdp description *peer-address*
default ip msdp description *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer
text	Descriptive information for MSDP peer

Defaults No descriptive information is configured for MSDP peer.

Command Mode Global configuration mode

Usage Guide The administrator can configure descriptive information for MSDP peers in order to identify them conveniently.
If the descriptive information A is specified for an MSDP peer, A is displayed. If no descriptive information is specified, “No description” is displayed.

Configuration Examples The following example configures the descriptive information for peer 172.17.1.2 as "customer-a".

```
Ruijie(config)# ip msdp description 172.171.1.2 customer-a
```

Related Commands

Command	Description
show ip msdp peer	Displays the descriptive information for MSDP peer.

Platform Description This command is supported only on L3 devices.

ip msdp filter-sa-request

Use this command to filter the SA request messages sent from MSDP peer.
Use the **no** or **default** form of this command to restore the default setting.
ip msdp filter-sa-request *peer-address* [**list** *access-list*]
no ip msdp filter-sa-request *peer-address*
default ip msdp filter-sa-request *peer-address*

Parameter

Parameter	Description

Description

peer-address	IP address of the MSDP peer
list *access-list*	The standard IP access list number or name for limiting multicast group addresses

Defaults All SA request messages from MSDP peer will be accepted and replied.

Command Mode Global configuration mode

Usage Guide Use this command to control which SA request messages will be accepted and replied.
If no access list is specified, all SA request messages will be ignored.
If a null access list is specified, all SA request messages will be ignored.
If an access list is specified, only the SA request messages from the multicast group permitted by the access list will be accepted, and other messages will be ignored.

Configuration Examples The following example configures to filter SA request messages from peer 172.16.223.1 and only accept SA request messages with group address falling within 224.0.1.0-224.0.1.255.

```
Ruijie(config)# ip msdp filter-sa-request 172.16.223.1 list 1
Ruijie(config)# access-list 1 permit 224.0.1.1 0.0.0.255
```

Related Commands

Command	Description
ip msdp peer	Creates MSDP peer.

Platform Description This command is supported only on L3 devices.

ip msdp mesh-group

Use this command to configure a MSDP peer to be a member of a mesh group.
Use the **no** form of this command to remove the configuration.
Use the **default** form of this command to restore the default settings.
ip msdp mesh-group *mesh-name peer-address*
no ip msdp mesh-group *mesh-name peer-address*
default ip msdp mesh-group *mesh-name peer-address*

Parameter Description

Parameter	Description
mesh-name	Name of mesh group, case sensitive
peer-address	IP address of the MSDP peer to be a member of mesh group.

Defaults No mesh group will be created, and MSDP peers do not belong to any mesh group.

Command Mode Global configuration mode

Usage Guide All MSDP peers in the mesh group shall be fully meshed, namely MSDP peer relationship has been established between every two members in the mesh group.
The SA received by one member of the mesh group won't be forwarded to other members in the same mesh group, thus reducing SA flooding and simplify Peer-RPF forwarding.

Configuration Examples The following example configures MSDP peer at address 192.168.1.3 to be a member of the mesh group named "msdp-mesh".

```
Ruijie(config)# ip msdp mesh-group msdp-mesh 192.168.1.3
```

Related Commands

Command	Description
show ip msdp mesh-group	Displays the information of mesh group.

Platform Description This command is supported only on L3 devices.

ip msdp originator-id

Use this command to allow a speaker that originates a SA message to use the IP address of the interface as the originator address in the SA message.
Use the **no** form of this command to remove this configuration.
Use the **default** form of this command to restore the default setting.
ip msdp originator-id *interface-type interface-number*
no ip msdp originator-id
default ip msdp originator-id

Parameter Description

Parameter	Description
interface-type	Interface type
interface-number	Interface number

Defaults By default, the originator address in SA messages will be the RP address configured by PIM.

Command Mode Global configuration mode

Usage Guide The master IP address of this interface will be used as the originator address in the SA messages. If no IP address is configured for this interface, or the interface is shut down, then the originator address in the SA messages won't use the master IP address of this interface, but use the RP address configured by PIM.
Under certain circumstances, you may expect to change the originator address in SA messages,

such as during Anycast-RP deployment. By this time, you can use this command to modify the originator address in SA messages.

Configuration Examples The following example uses the IP address of Loopback0 as the RP address in SA messages.

```
Ruijie(config)# ip msdp originator-id loopback0
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

ip msdp password

Use this command to enable MD5 encryption of the TCP connection between MSDP peers.
Use the **no** or **default** form of this command to restore the default setting.
ip msdp password peer *peer-address* [*encryption-type*] *string*
no ip msdp password peer *peer-address*
default ip msdp password peer *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer
encryption-type	Grade of password: 0 (lowest level)-7 (highest level). Currently, only 0 and 7 are supported. The default encryption type is 0.
string	The password used for TCP MD5 authentication. Range: up to 80 characters when the encryption type is 0; up to 160 characters when the encryption type is 7.

Defaults MD5 encryption of the TCP connection between MSDP peers is disabled.

Command Mode Global configuration mode

Usage Guide When it is needed to authenticate the MSDP peers, you can enable MD5 encryption of TCP connection between MSDP peers. In such a case, two interconnected MSDP peers must be configured with MD5 authentication with same password, or else the connection will fail.
If the password is configured or changed, the local MSDP device won't terminate the current session, but will try to use the new password to maintain the current session until timeout.
If you have configure the password locally for the MSDP peer but no password is configured on MSDP, the following warning message will be displayed on the console:

```
%TCP-6-BADAUTH: MD5 digest NOT expected but found (200.200.200.6, 39996)->(200.200.200.16, 639)
```

If different MD5 passwords are configured between MSDP peers, the following warning message will be displayed on the console:

```
%TCP-6-BADAUTH: MD5 digest failed for (200.200.200.6, 12302)->(200.200.200.16, 639)
```


Caution

If the encryption type is 0, the encryption key for TCP is the string entered in the console. That is, this type of encryption is supported when Ruijie Networks MSDP devices communicates with those from other vendors. Thus, this encryption type is recommended for mutual communication between devices from different vendors.


Caution

If the encryption type is 7, the entered encryption key must be even and not less than 4. Different from type 0, the encryption key is not the string entered in the console. Instead, it is a new string computed by Ruijie-defined algorithm. In addition, our algorithm is different from other private vendor-specific algorithms. Therefore, this encryption type is supported only when Ruijie Networks devices are mutually connected.

Configuration Examples The following example configures the MD5 password of "test" for the MSDP peer of 10.32.43.144.

```
Ruijie(config)# ip msdp password peer 10.32.43.144 0 test
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

ip msdp peer connect-source

Use this command to create MSDP peer.

Use **no** or **default** form of this command to remove MSDP peer.

ip msdp peer *peer-address* **connect-source** *interface-type interface-number*

no ip msdp peer *peer-address*

default ip msdp peer *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer The peer MSDP device uses this address to communicate with the local MSDP device for TCP connection.
interface-type *interface-number*	Interface type and interface number. The local MSDP device uses the main address of this interface as the

	source IP for the TCP connection to the remote MSDP peer. Loopback interface is recommended. If no IP address is configured for this interface, or the interface is shut down, then MSDP peer relation cannot be established.

Defaults No MSDP peer is created.

Command Mode Global configuration mode

Usage Guide To enable MSDP, MSDP peer must be created.

Configuration Examples The following example configures the main address of interface loopback 0 as the source address for establishing MSDP peer relation with 192.168.5.1.

```
Ruijie(config)# ip msdp peer 192.168.5.1 connect-source loopback 0
```

Related Commands

Command	Description
show ip msdp peer	Displays the information about MSDP peer.

Platform Description This command is supported only on L3 devices.

ip msdp redistribute

Use this command to configure which (S, G) entries from the multicast routing table can be advertised to MSDP peers.
Use the **no** form of this command to remove this configuration.
Use the **default** form of this command to restore the default settings.
ip msdp redistribute [**list** *access-list-name*] [**route-map** *route-map*]
no ip msdp redistribute
default ip msdp redistribute

Parameter Description

Parameter	Description
list *access-list-name*	Number or name of an extended IP access list that controls which multicast routes (S, G) can be advertised.
route-map *route-map*	Defines route-map.

Defaults All multicast sources (S, G) registered on the local RP will be advertised.

Command Global configuration mode

Mode

Usage Guide After redistribution filtering is configured, the (S, G) information from the local AS or the other AS can be added to the MSDP only through redistribution filtering.
If "**list** *access-list-name*" is specified, only those matched multicast routes (S, G) will be advertised.
If "**route-map** *map-name"* is specified, only multicast routes (S, G) matching the criteria given in "map-name" will be advertised.
If two keywords are specified, then multicast routes (S, G) matching all conditions will be advertised.
If the "**ip msdp redistribute**" command is configured with no keywords, no multicast sources will be advertised.

Configuration Examples The following example configures to only advertise multicast routes with multicast source being 200.200.200.0/24 and group address being 225.1.1.0/24.

```
Router(config)# ip msdp redistribute list 100
Router(config)# ip access-list extended 100
Router(config-ext-nacl)#  permit  ip  200.200.200.0  0.0.0.255  225.1.1.0
0.0.0.255
```

Related Commands

Command	Description
ip msdp sa-filter in	Configures the incoming filter for SA messages.
ip msdp sa-filter out	Configures the outgoing filter for SA messages.

Platform Description This command is supported only on L3 devices.

ip msdp sa-filter in

Use this command to configure an incoming filter for SA messages.
Use the **no** or **default** form of this command to remove the incoming filter.
ip msdp sa-filter in *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*]
no ip msdp sa-filter in *peer-address*
default ip msdp sa-filter in *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer
list *access-list*	Number or name of an extended IP access list that controls which multicast routes (S, G) can be received.
route-map *route-map*	Specify the name of route-map; only SA messages matching the criteria given in "map-name" can pass through.
rp-list *rp-access-list*	Number or name of standard access list that controls RPs.
rp-route-map *rp-route-map*	Specify the name of route map for RP; only the SA messages

	matching rp-map-name can be accepted.

Defaults All incoming SA messages will be accepted without filtering.

Command Mode Global configuration mode

Usage Guide If the command is configured, but no access list or route map is specified, all incoming SA messages will be filtered.
If only the **list** keyword or the **route-map** keyword is used, the multicast source (S, G) in SA messages matching the criteria corresponding to this keyword will be accepted.
If only the **rp-list** keyword or the **rp-route-map** keyword is used, the SA message will be accepted if the RP address carried in SA message matches the criteria corresponding to this keyword.
If two or more keywords of **list, route-map, rp-list** and **rp-route-map** are used, the SA message will be accepted if any multicast source (S, G) in SA message meet the criteria corresponding to all keywords.

Configuration Examples The following example configures that all SA messages from the peer of 10.234.1.43 will be filtered.

```
Ruijie(config)# ip msdp peer 10.234.1.43
Ruijie(config)# ip msdp sa-filter in 10.234.1.43
```

Related Commands

Command	Description
ip msdp peer	Configures MSDP peer.
ip msdp sa-filter-out	Configures the outgoing filter for SA messages received from MSDP peers.

Platform Description This command is supported only on L3 devices.

ip msdp sa-filter out

Use this command to configure an outgoing filter for SA messages.
Use the **no** or **default** form of this command to remove the outgoing filter.
ip msdp sa-filter out *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*]
no ip msdp sa-filter out *peer-address*
default ip msdp sa-filter out *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of MSDP peer
list *access-list*	Number or name of an extended IP access list that controls which multicast routes (S, G) can be received.

route-map *route-map*	Specify the name of route-map; only SA messages matching the criteria given in "map-name" can pass through.
rp-list *rp-access-list*	Number or name of standard access list that controls RPs.
rp-route-map *rp-route-map*	Specify the name of route map for RP; only the SA messages matching rp-map-name can be accepted.

Defaults All SA messages received will be forwarded to the MSDP peer.

Command Mode Global configuration mode

Usage Guide If the command is configured, but no access list or route map is specified, all SA messages won't be forwarded to this MSDP peer.
If only one keyword of **list, route-map, rp-list** and **rp-route-map** is used, the multicast source pair (S, G) will be forwarded to this MSDP peer if the criteria corresponding to this keyword are met.
If two or more keywords of **list, route-map, rp-list** and **rp-route-map** are used, the (S, G) pair will only be forwarded to this MSDP peer if criteria corresponding to all keywords are met.

Configuration Examples The following example allows only multicast sources that pass access list 100 to be forwarded to the peer of 10.234.1.43.

```
Ruijie(config)# ip msdp peer 10.234.1.43
Ruijie(config)# ip msdp sa-filter out 10.234.1.43 list 100
Ruijie(config)# access-list 100 permit ip 10.211.0.0 0.0.255.255 224.12.0.0
0.0.255.255
```

Related Commands

Command	Description
ip msdp peer	Configures MSDP peer.
ip msdp sa-filter-in	Configures the incoming filter for SA messages received from MSDP peers.

Platform Description This command is supported only on L3 devices.

ip msdp sa-limit

Use this command to configure the allowable maximum number of Source-Active (SA) cache entries from a MSDP peer.
Use the **no** or **default** form of this command to restore the default settings.
ip msdp sa-limit *peer-address sa-limit*
no ip msdp sa-limit *peer-address*
default ip msdp sa-limit *peer-address*

Parameter

Parameter	Description

Description

peer-address	IP address of MSDP peer
sa-limit	Maximum number of SA messages from an MSDP peer allowed in the SA cache

Defaults The maximum number of SA messages from an MSDP peer allowed in the SA cache is not limited.

Command Mode Global configuration mode

Usage Guide It is suggested to configure this command on all MSDP peers to prevent SA flooding attacks from MSDP peers.
When the local device has learned A (quantity) SA entries from an MSDP peer, and A is greater than B (the SA limit), the SA entries from this peer will not be cleared at once. Instead, the aging mechanism (no more than 135 seconds) will lower A to B. That is, this command is not effective immediately. It aims to saving effective multicast information best to raise networking productivity. If you want to clear the SA entries in such case, use the **clear ip msdp sa-cache** command.

Configuration Examples The following example configures the SA message limit to 100 for the MSDP peer with IP address being 172.16.3.1.

```
Ruijie(config)# ip msdp sa-limit 172.16.3.1 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

ip msdp shutdown

Use this command to shut down the connection to MSDP peer.
Use the **no** or **default** form of this command to restore the default settings.
ip msdp shutdown *peer-address*
no ip msdp shutdown *peer-address*
default ip msdp shutdown *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer

Defaults The connection to peer is not shut down.

Command Global configuration mode

Mode

Usage Guide Only the TCP connection to the specified MSDP peer will be shut down. Neither the MSDP peer nor its configurations will be cleared.

Configuration Examples The following example shuts down the MSDP peer at IP address 192.168.7.20.

```
Ruijie(config)# ip msdp shutdown 192.168.7.20
```

Related Commands

Command	Description
ip msdp peer	Creates MSDP peer.

Platform Description This command is supported only on L3 devices.

ip msdp timer

Use this command to configure the interval for timer re-connection.
Use the **no** or **default** form of this command to restore the default settings.
ip msdp timer *interval*
no ip msdp time
default ip msdp timer

Parameter Description

Parameter	Description
interval	Interval for timer re-connection, within the range from 1 to 60 in the unit of seconds

Defaults The default interval is 30 seconds.

Command Mode Global configuration mode

Usage Guide By default, the interval for timer re-connection is 30 seconds, that is, the peer in active end can initiate only one TCP connection within 30 seconds. In certain applications, the interval is expected to be decreased in order to accelerate convergence of MSDP peering relation.

Configuration Examples The following example sets the interval for timer re-connection to 20 seconds.

```
Ruijie(config)# ip msdp timer 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

ip msdp ttl-threshold

Use this command to limit the TTL value of multicast data packets carried in SA messages in order to limit the transmission of multicast packets.
Use the **no** or **default** form of this command to restore to the default settings.
ip msdp ttl-threshold *peer-address ttl-value*
no ip msdp ttl-threshold *peer-address*
default ip msdp ttl-threshold *peer-address*

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer
ttl-value	TTL value in the range from 0 to 255

Defaults TTL threshold is 0 by default.

Command Mode Global configuration mode

Usage Guide This command limits multicast data packets which are sent in data-encapsulated SA messages. Only multicast packets with an IP-header TTL greater than or equal to the ttl-value will be sent to the MSDP peer. If the TTL value of multicast data is less than the threshold configured, then the multicast data will be separated from SA messages and discarded, and the SA messages without multicast data will be sent to the MSDP peer.
This command only limits the transmission of multicast data in SA messages without compromising the transmission of multicast sources in SA messages

Configuration Examples The following example configures the TTL threshold for peer at IP address 192.168.10.1 to 8 hops:

```
Ruijie(config)# ip msdp ttl-threshold 192.168.10.1 8
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

show ip msdp count

Use this command to display the number of sources and groups originated in SA messages and the

number of SA messages from an MSDP peer in the SA cache.

show ip msdp count [*as-number*]

Parameter Description

Parameter	Description
as-number	Displays the number of sources and groups originated in SA messages from the specified autonomous system number.

Defaults N/A

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

Usage Guide N/A

Configuration Examples

```
Ruijie# sh ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
  1.1.1.2       : 0
  100.100.100.14 : 0
  100.100.100.15 : 0
  100.100.100.200: 0
  200.200.200.2 : 2
  200.200.200.3 : 0
  200.200.200.6 : 0
  200.200.200.13 : 0
  200.200.200.66 : 0
SA State per ASN Counters, <asn>: <# sources>/<# groups>
Total entries: 2
100: 1/2   .
```

Field	Description
200.200.200.200:2	MSDP peer with IP address 200.200.200.200; 2 SA messages in the SA cache.
Total entries	Total number of SA entries in the SA cache.
?:1/2	Unknown autonomous system: 1 source address/2 multicast group addresses

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

show ip msdp mesh-group

Use this command to display the information of mesh group.

show ip msdp mesh-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

```
Ruijie# sh ip msdp mesh-group
MSDP peers in each Mesh-group,<Mesh-group name>:<# peers>
msdp-mesh
  1.1.1.2
  1.1.1.3
```

Field	Description
msdp-mesh	Name of mesh group
1.1.1.2	One MSDP peer under this mesh group.

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

show ip msdp peer

Use this command to display detailed information about the MSDP peer.

show ip msdp peer [*peer-address*]

Parameter Description

Parameter	Description
peer-address	IP address of the MSDP peer

Defaults N/A

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

Usage Guide N/A

Configuration Examples

```
Ruijie#show ip msdp peer 20.0.0.1
MSDP PEER 20.0.0.1 (No description), AS unknown
  Connection status:
    State: Listen, Resets: 1, Connection source: GigabitEthernet 0/1 (20.0.0.2)
    Uptime(Downtime): 00:00:25, Message sent/received: 13/19
    Input messages discarded: 0
    Connection and counters cleared 00:13:25 ago
    Local Address of connection: 20.0.0.2
    MD5 signature protection on MSDP TCP connection: enabled
  SA Filtering:
    Input (S,G) Access-list filter: None
    Input (S,G) route-map filter: None
    Input RP Access-list filter: None
    Input RP Route-map filter: None
    Output (S,G) Access-list filter: None
    Output (S,G) Route-map filter: None
    Output RP Access-list filter: None
    Output RP Route-map filter: None
  SA-Requests:
    Input filter: None
  Peer ttl threshold: 0
  SAs learned from this peer: 2, SAs limit: No-limit
  Message counters:
    SA messages discarded: 0
    SA messages in/out: 13/0
    SA Requests discarded/in: 0/0
    SA Responses out: 0
    Data Packets in/out: 6/0
```

Field	Description
MSDP Peer	IP address of MSDP peer.
AS	Autonomous system to which the MSDP peer belongs. If it is an unknown AS, “unknown” will be displayed.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the source address for TCP connection.
Uptime(Downtime):	Up time/down time of MSDP peer.
Messages sent/received:	Number of SA messages received.

SA Filtering:	SA filtering information.
SAs learned from this peer:	Number of SA entries learned from MSDP peer.
SAs limit:	SA message limit for this MSDP peer.

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on L3 devices.

show ip msdp rpf-peer

Use this command to display the information about MSDP RPF peer corresponding to the specified originator address.

show ip msdp rpf-peer *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address of the originator of SA messages

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 rpf-peer information of RP at address 1.1.1.1:

```
Ruijie# sh ip msdp rpf-peer 1.1.1.1
RPF peer information for 1.1.1.1
RPF peer: 200.200.200.2
RPF rule: Peer is only active peer
RPF route/mask: Not-used
RPF type: Not-used
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is only supported on L3 devices.

MPLS Configuration Commands

Basic MPLS Commands

advertise-labels

Use this command to configure the policy for distributing a label to an IP route Forwarding Equivalence Class (FEC). Use the **no** form of this command to restore the default value.

advertise-labels [**for host-routes** | **for bgp-routes** [**acl** *acl_name*]| **for default-route | for acl** *prefix-access-list* [**to** *peer-access-list*]

[**no**] **advertise-labels** [**for host-routes** | **for bgp-routes** [**acl** *acl_name*]| **for default-route | for acl** *prefix-access-list* [**to** *peer-access-list*]

Parameter description

Parameter	Description
for host-routes	(Optional) Distributes labels to host routes (the subnet mask is 32 bits long) only.
for bgp-routes [acl *acl_ame*]	(Optional) Distributes labels to BGP routes only. You can distribute labels to only the BGP routes that meet conditions by using ACL keywords.
for default-route	(Optional) Distributes non-3 labels to default routes.
for acl *prefix-access-list*	(Optional) Specifies the prefix of the routes to which labels are distributed.
to *peer-access-list*	(Optional) Specifies the neighbors to which label binding information is sent.

Defaults

Labels are distributed to all LDP neighbors by default.
Labels are distributed to all IGP routes instead of BGP routes by default. In addition, FTN is not added to BGP routes.
Implicit null label 3 is distributed to default routes by default.

Command mode

config-mpls-router mode

Usage guidelines

This command is effective to only the IP route FEC instead of other FECs such as PW FEC. Use the **advertise-labels for acl** *fec_acl* **to** *peer_acl* command to specify the FECs and LDP peers to which labels are distributed. If *fec_acl* is specified, only one rule can be configured. For the same *peer-acl*, multiple rules can be configured. If this command is configured but no filtering rule is configured in the corresponding ACL, it is equivalent that this command is not configured, that is, FEC label mapping messages are sent normally. A label request received by an LDP session

working in DOD mode cannot be replied with a label mapping message if the request does not meet the label distribution policy as a result of the configured rule. Even if the rule is cancelled afterwards, the request that has been filtered cannot be distributed with a label mapping message. In this case, you can use the **clear mpls ldp neighbor** command to reset the LDP session. You can use this command to configure a maximum of 64 rules.

Use the **advertise-labels for bgp-routes** command to distribute labels to BGP routes. You can use this command with the *acl* option to distribute labels to BGP routes that meet conditions or use this command without the *acl* option to distribute labels to all BGP routes. Use the **no advertise-labels for bgp-routes** command to disable the distribution of labels to BGP routes. Note that the distribution of labels to BGP routes is still controlled by the label distribution policy of LDP. Use the **advertise-labels for host-routes** command to distribute labels to only route prefixes with 32-bit masks (namely host routes).

Use the **advertise-labels for default-route** command to distribute non-3 labels to default routes, thus establishing an LSP for default routes.

Caution

Labels are distributed to all FECs by default. Therefore, you must use the **no advertise-labels** command to disable the distribution of labels to all FECs if you want to distribute labels to only the FECs that meet specified ACL rules. In this manner, labels are not distributed to those FECs that do not meet ACL rules.

After the **no advertise-labels** command is configured, labels are distributed to only the FECs that meet **advertise-labels for acl** *prefix-access-list* [**to** *peer-access-list*] and instead of other FECs. If the preceding rule is not met, labels are not distributed to BGP routes and host routes even if the **advertise-labels for bgp-routes** command or **advertise-labels for host-routes** command is configured.

When the **advertise-labels for host-routes** command is configured, LDP distributes labels to only host routes and adds FTN to only host routes.

Examples

1) The following example enables the LDP instance to distribute labels to the host route FEC only.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# advertise-labels for host-routes
```

2) The following example enables the LDP instance not to distribute any label to the LDP peer of the IP route FEC.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# no advertise-labels
```

3) The following example enables the LDP instance to distribute labels to all LDP peers of the FEC with 192.168.0.0/16 as the route prefix.

```
Ruijie(config)#ip access-list standard fec_acl
Ruijie(config-std-nacl)#permit 192.168.0.0 0.0.255.255
Ruijie(config-std-nacl)# exit
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# no advertise-labels
Ruijie(config-mpls-router)# advertise-labels for acl fec_acl
```

4) The following example enables the LDP instance to distribute labels to LDP peer 6.6.6.6 and

LDP peer 7.7.7.7 of the FEC with 192.168.0.0/24 as the route prefix, and to all LDP peers of other FECs.

```
Ruijie(config)#ip access-list standard fec_acl
Ruijie(config-std-nacl)#permit 192.168.0.0 0.0.0.255
Ruijie (config)#ip access-list standard peer_acl
Ruijie (config-std-nacl)#permit host 6.6.6.6
Ruijie (config-std-nacl)#permit host 7.7.7.7
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# advertise-labels for acl fec_acl to peer_acl
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

backoff

Use this command to configure the time for LDP exponential backoff. Use the **no** form of this command to restore the default value.

backoff *initial-backoff maximum-backoff*

no backoff

Parameter description

Parameter	Description
initial-backoff	Indicates the initial time in seconds of exponential backoff. The range is from 5 to 2147483. The default value is 15.
maximum-backoff	Indicates the maximum time in seconds of backoff. The range is from 5 to 2147483. The default value is 120.

Defaults The initial time of exponential backoff is 15 seconds and the maximum time is 120 seconds by default.

Command mode **config-mpls-router** mode

Usage guidelines When the LSR acts as the active side, an LDP session cannot be established if the parameters for negotiation are found inconsistent during establishment of the LDP session. In this case, the LSR continuously attempts to re-establish an LDP session, which wastes system resources. The exponential backoff mechanism is used to prevent the active side from attempting to re-establish an LDP session continuously. The active side attempts to re-establish an LDP session only when the backoff time expires or the CSN of the Help message from the peer changes (which means changes in the configuration of the peer).

Examples The following example sets the initial time of exponential backoff to 20 seconds and the maximum time to 300 seconds in this instance.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# advertise-labels for bgp-routes
```

Related commands	**Command**	**Description**
	show mpls ldp parameters	Shows the configuration parameters of the LDP instance.
Platform description	N/A	

clear mpls ldp neighbor

Use this command to forcibly disconnect an LDP session and re-establish an LDP session.

clear mpls ldp neighbor [**all** | **vrf** *vrf-name*] {* | *ip-address*}

Parameter description	**Parameter**	**Description**
	all	Forcibly disconnects LDP sessions under all virtual routing and forwarding instances (VRFs, including the default global VRF) and re-establishes sessions.
	vrf *vrf-name*	Forcibly disconnects LDP sessions under specified VRFs and re-establishes sessions.
	*	Forcibly disconnects LDP sessions under specified VRFs or all VRFs and re-establishes sessions.
	ip-address	Forcibly disconnects LDP sessions established between specified VRFs or all VRFs and specified LDP peers and re-establishes sessions.

Defaults N/A

Command mode Privileged mode

Usage guidelines If no VRF is specified in this command, it indicates that LDP sessions under the default global VRF are forcibly reset.

Examples 1) The following example forcibly resets all established LDP sessions under the default global VRF.

```
Ruijie# clear mpls ldp neighbor *
```

The following example forcibly resets the LDP sessions established between the default global VRF and the peer 10.10.10.10.

```
Ruijie# clear mpls ldp neighbor 10.10.10.10
```

2) The following example forcibly resets the LDP sessions established under all VRFs (including default global VRF).

```
Ruijie# clear mpls ldp neighbor all *
```

Related commands

Command	Description
show mpls ldp neighbor	Shows the state of an LDP session.

Platform description N/A

discovery targeted-hello

Use this command to set the holdtime or interval for the extended peer Hello message. Use the **no** form of this command to restore the default value.

discovery targeted-Hello {**holdtime|interval**} *seconds*

no discovery targeted-Hello {**holdtime|interval**}

Parameter description

Parameter	Description
holdtime	Specifies the holdtime of the Hello message for the extended mechanism.
interval	Specifies the interval of the Hello message for the extended mechanism.
seconds	The range is from 1 to 65535. Holdtime 65535 indicates that the Hello message will never time out.

Defaults By default, the holdtime of the Hello message for the extended mechanism is 45 seconds, and the interval of the Hello message is 5 seconds, which is 1/9 of the holdtime.

Command mode **config-mpls-router** mode

Usage guidelines During configuration, ensure that the holdtime of the target Hello is greater than the interval value. Otherwise, LDP cannot work normally according to the requirement. Note that this command is valid for only the targeted Hello used by the extended discovery mechanism.

Examples

```
Ruijie(config)# mpls route ldp
Ruijie(config-mpls-router)# discovery target-Hello holdtime 90
```

Related commands

Command	Description
show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.

Platform description	N/A	

discovery targeted-hello accept

Use this command to enable the LDP to accept all targeted Hello packets or the targeted Hello packets from the neighbor matching the specified ACL. Use the **no** form of this command to remove the configuration.

discovery targeted-hello accept [**from** *acl-name*]

no discovery targeted-hello accept

Parameter description

Parameter	Description
N/A	N/A

Defaults LDP accepts only the targeted Hello packets from the peer end by default.

Command mode config-mpls-router mode

Usage guidelines Configure the neighbor on the local end and enable this function on the peer end. You can delete the peer end by deleting the neighbor configuration on the local end.

Examples The following example enables LDP to accept all targeted Hello packets from the peer end.

```
Ruijie#config terminal
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#discovery targeted-hello accept
```

The following example enables LDP to accept the targeted Hello packets from neighbor 1.1.1.1.

```
Ruijie#config terminal
Ruijie(config)#ip access-list standard target_acl
Ruijie(config-std-nacl)#permit host 1.1.1.1
Ruijie(config-std-nacl)#exit
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#discovery targeted-hello accept from
target_acl
```

Related commands

Command	Description
N/A	N/A

Platform description	N/A

explicit-null

Use this command to configure the distribution of explicit null labels to direct routes or direct route prefixes that meet specified ACL rules, or the distribution of explicit null labels to only the neighbors that meet rules and of implicit null labels to other neighbors. Use the **no** form of this command to cancel relevant configurations.

explicit-null [for *prefix-acl*] **[to** *peer-acl* **]**

no explicit-null

Parameter description

Parameter	Description
for prefix-acl	(Optional) Specifies the prefixes of direct routes whose implicit null labels are replaced by explicit null labels.
to peer-acl	(Optional) Specifies the LDP peers whose implicit null labels can be replaced by explicit null labels.

Defaults

Implicit null labels are distributed to direct routes for all peers by default.

Command mode

config-mpls-router mode

Usage guidelines

Note

1. When the LSP of the FEC to which a direct route corresponds serves as the bearer tunnel of an L2 VPN or an L3 VPN, an explicit null label cannot be distributed to the corresponding FEC of this direct route.
2. If a command is configured to distribute explicit null labels but no filtering rule is configured in the corresponding ACL, it is equivalent that the command is not configured, that is, implicit null labels are distributed to direct routes for all neighbors.
3. This command can be configured for only global LDP instances, and VRFs do not support this command.

Examples

1) The following example enables the LDP to distribute explicit null labels to all direct routes by LDP. In this example, no parameter is specified.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# explicit-null
```

2) The following example enables the LDP to distribute explicit null labels to LDP peer 1.1.1.1 for direct routes with 192.168.0.0/16 as the prefix. Otherwise, the LDP distributes implicit null labels.

```
Ruijie(config)#ip access-list standard fec_acl
```

```
Ruijie(config-std-nacl)#permit 192.168.0.0 0.0.255.255
Ruijie(config-std-nacl)#exit
Ruijie(config)#ip access-list standard peer_acl
Ruijie(config-std-nacl)#permit host 1.1.1.1
Ruijie(config-std-nacl)#exit
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# explicit-null for fec_acl to peer_acl
```

Related commands	Command	Description
	N/A	N/A

Platform description N/A

ignore ipv6-adj negotiation

Use this command to ignore IPv6 adjacency negotiation. Use the **no** form of this command to remove the configuration.

ignore ipv6-adj negotiation [**to** *peer-access-list*]

no ignore ipv6-adj negotiation

Parameter description	Parameter	Description
	to *peer-access-list*	Specifies the neighbor for IPv6 adjacency negotiation.

Defaults IPv6 adjacency negotiation is enabled by default.

Command mode config-mpls-router mode

Usage guidelines N/A

Examples The following example ignores IPv6 adjacency negotiation.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# ignore ipv6-adj negotiation
```

Related commands	Command	Description
	N/A	N/A

Platform description N/A

inter-area-lsp

Use this command to configure inter-area LSP. Use the **no** form of this command to remove the configuration.

inter-area-lsp [**for acl** *acl_name*]

no inter-area-lsp

Parameter description

Parameter	Description
for acl *acl_name*	(Optional) Specifies an ACL list.

Defaults

Inter-area LSP is disabled by default.

Command mode

config-mpls-router mode

Usage guidelines

Examples

The following example enables inter-area LSP.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# inter-area-lsp
```

The following example enables inter-area LSP for VRF instance vpna.

```
Ruijie(config)# ip access-list standard acl_1
Ruijie(config-std-nacl)# permit host 192.166.1.1
Ruijie(config-std-nacl)# exit
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# inter-area-lsp for acl acl_1
```

The following example enables inter-area LSP for 192.166.1.1/32.

```
Ruijie(config)# ip access-list standard acl_1
Ruijie(config-std-nacl)# permit host 192.166.1.1
Ruijie(config-std-nacl)# exit
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# inter-area-lsp for acl acl_1
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

ipv4|ipv6 gtsm-protection

Use this command to enable GTSM protection for the specified address family. Use the **no** form

of this command to remove the configuration.

{ **ipv4 | ipv6** } **gtsm-protection**

no { **ipv4 | ipv6** } **gtsm-protection**

Parameter description

Parameter	Description
ipv4	Specifies an IPv4 address family.
ipv6	Specifies an IPv6 address family.

Defaults GTSM protection is enabled for all address families.

Command mode config-mpls-router mode

Usage guidelines Run the **enable GTSM protection** command to enable GTSM protection and run the **neighbor valid-hops** command to configure the number of GTSM protection hops.

Examples The following example disables GTSM protection for the specified address family.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# no ipv4 gtsm-protection
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

ipv6 neighbor

Use this command to configure an LDP IPv6 peer end. Use the **no** form of this command to remove the configuration.

ipv6 neighbor *ipv6-address*

no ipv6 neighbor *ipv6-address*

Parameter description

Parameter	Description
ipv6-address	Specifies the IPv6 address of the peer end.

Defaults No LDP IPv6 peer end is configured by default.

Command mode config-mpls-router mode

Usage guidelines To establish an LDP extended session, configure the peer end on both ends. Alternatively, configure the peer end on one end and configure **discovery target-hello accept** command on the other end.

Examples The following example configures LDP IPv6 peer end 2002::2.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# ipv6 neighbor 2002::2
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

ipv6 transport-address

Use this command to configure an IPv6 transmission address for an LDP session. Use the **no** form of this command to remove the configuration.

ipv6 transport-address { *ipv6-address* | *interface-name* }

no ipv6 transport-address

Parameter description

Parameter	Description
ipv6-address	Specifies an global IPv6 transmission address for an LDP session
interface-name	Specifies an interface IPv6 transmission address for an LDP session.

Defaults N/A

Command mode config-mpls-router mode

Usage guidelines If you want to configure the **ipv6 transport-address** *interface-name* command, make sure that the interface is configured with an IPv6 transmission address

The IPv6 transmission address must be configured manually. Otherwise, the local end will not send LDP IPv6 Hello packets.

Examples The following example configures an interface for an LDP session.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# ipv6 transport-address loopback0
```

Related commands

Command	Description
N/A	N/A

Platform description	N/A

label-merge

Use this command to enable the global label merge function. Use the **no** form of this command to disable this function.

label-merge

[**no**] **label-merge**

Defaults The global label merge function is enabled by default.

Command mode **config-mpls-router** mode

Usage guidelines Use this command to enable the global label merge function.

This command is valid for only the DOD label distribution mode instead of the DU label distribution mode. That is, when an LDP session is in DU label distribution mode, the LDP session uses the label merge function on matter whether this function is enabled or disabled.

All LDP sessions are reset when this command is confiugred to enable or disable the label merge function.

Examples

```
Ruijie(config)# mpls route ldp
Ruijie(config-mpls-router)# label-merge
```

Related commands

Command	Description
show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.
mpls ldp distribution-mode	Configures the label distribution mode used for each interface.

Platform description N/A

label-retention-mode

Use this command to set the label retention mode. Use the **no** form of this command to restore the default value.

label-retention-mode {liberal | conservative}

label-retention-mode

[no] label-retention-mode

Parameter

Parameter	Description

description	**liberal**	Uses the liberal label retention mode.
	conservative	Uses the conservative label retention mode.

Defaults The liberal label retention mode is used by default.

Command mode **config-mpls-router** mode

Usage guidelines This command is invalid for only FEC label mapping messages that are received from neighbors after configuration of this command.

Examples

```
Ruijie(config)# mpls route ldp
Ruijie(config-mpls-router)# label-retention-mode liberal
```

Related commands	**Command**	**Description**
	show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.
Platform description	N/A	

label-switching

Use this command to enable the interface to forward the MPLS label messages.

[**no**] **label-switching**

Defaults The MPLS label message forwarding function is disabled for an interface by default.

Command mode Interface configuration mode

Usage guidelines Configure the **label-switching** command to enable an interface to forward MPLS packets.

Examples

```
Ruijie(config)# interface Gi4/1
Ruijie(config-if)# label-switching
```

Related commands	**Command**	**Description**
	show mpls label-pool	Shows the usage of the label pool in each label space
	show mpls summary	Shows the interfaces on which the label forwarding capability is enabled.
	mpls ip (Interface configuration mode)	Enables the LDP function of an interface.

Platform description N/A

ldp router-id

Use this command to set the router ID of the LDP. Use the **no** form of this command to restore the default value, which does not take effect immediately.

ldp router-id { *ip-address* **| interface** *interface-name* **[force]}**

no ldp router-id

Parameter description

Parameter	Description
ip-address	Specifies a static IP address as the router ID of LDP. It takes effect immediately after being configured.
interface-name [**force**]	Configures the primary address of a specified interface as the router ID of LDP. If the force keyword is specified, the new router ID is forced to take effect immediately. Otherwise, the new router ID will not take effect immediately.

Defaults The system router ID is used as the LDP router ID by default.

Command mode **config-mpls-router** mode

Usage guidelines

If a static IP address is specified as the router ID of LDP and the address takes effect immediately after being configured, it indicates that the established session is disconnected and that a new router ID is used to re-establish a session.

If the IP address of a specified interface is specified as the router ID of LDP and the **force** keyword is not carried, the primary address of the currently configured interface is used as the new router ID only when the currently used router ID is unavailable. To use the address of an interface as the router ID, the following conditions must be met:

- The VRF to which the interface belongs must be the same as that to which LDP belongs.
- The interface must be in Up state.

Otherwise, the router ID cannot take effect even if the **force** keyword is specified. The router ID takes effect only when the preceding conditions are met and the **force** keyword is specified.

If a configured static IP address replaces a configured interface address to act as the router ID of LDP or vice versa, the router ID takes effect immediately. In this case, the LDP sessions established under the LDP instance are disconnected automatically and then re-established.

It is recommended that an interface address be used as the router ID of LDP. A static address is used to ensure compatibility with commands of earlier versions.

Examples

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# ldp router-id interface vlan 10 force
```

Related commands	Command	Description
	show mpls ldp parameter	Shows LDP configuration parameters under all or specified VRFs.
Platform description	N/A	

loop-detection

Use this command to enable loop detection. Use the **no** form of this command to disable loop detection.

loop-detection

[**no**]**loop-detection**

Defaults Loop detection is disabled by default.

Command mode config-mpls-router mode

Usage guidelines This command is valid for only LDP sessions of an LDP instance that are estalbished after configuration of this command.

Examples

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# loop-detection
```

Related commands	Command	Description
	show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.
	mpls ldp max-path-vector	Configures the maximum path vector allowed for LDP loop detection.
	mpls ldp max-hop-count	Configures the maximum hop count allowed for LDP loop detection.

Platform description N/A

lsp-control-mode

Use this command to set the LDP control mode globally. Use the **no** form of this command to restore the default value.

lsp-control-mode [**independent** | **ordered**]

no lsp-control-mode

Parameter description

Parameter	Description
independent	Uses the independent control mode.
ordered	Uses the ordered control mode.

Defaults The independent control mode is used by default.

Command mode config-mpls-router mode

Usage guidelines This command is valid for only label mapping messages of an established LDP session that are distributed after configuration of this command.

Examples This command sets the LDP control mode of the instance.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# lsp-control-mode ordered
```

Related commands

Command	Description
show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.

Platform description N/A

mpls ip (Global configuration mode)

Use this command to enable the MPLS forward function in global configuration mode. Use the **no** form of this command to disable this function.

mpls ip

no mpls ip

Parameter Description

Parameter	Description
N/A	N/A

Defaults The MPLS forward function is disabled by default.

Command mode Global configuration mode

Usage guidelines To implement MPLS forward, you must enable the MPLS globally firstly. The MPLS forward function is disabled by default. After the MPLS forward function is enabled, label forward is implemented first. IP forward is implemented only when label forward fails.

This command cannot be used to control the MPLS forward on a chip of the switch.

Examples

```
Ruijie(config)# mpls ip
```

Related commands

Command	Description
mpls ip	Enables the MPLS in interface configuration mode.

Platform description

N/A

mpls ip (Interface configuration mode)

Use this command to enable the LDP function in interface configuration mode. Use the **no** form of this command to disable the LDP function in interface configuration mode.

mpls ip

no mpls ip

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The LDP function is disabled by default.

Command mode

Interface configuration mode

Usage guidelines

The LDP function can be enabled on only an L3 interface. After the LDP function is enabled on an interface, you must use the label-switching command to enable the MPLS forward function.

For tunnel interfaces, the LDP function currently can be enabled on only the GRE tunnel.

Examples

```
Ruijie(config)# interface Gi4/1
Ruijie(config-if)# mpls ip
```

Related commands

Command	Description
mpls ldp hello-interval	Configures the interval for sending Hello messages.
label-switching	Enables the MPLS forward function in interface configuration mode.
mpls ldp hello-holdtime	Configures the Hello packet holdtime.

Platform description

N/A

mpls ipv6 (Interface configuration mode)

Use this command to enable LDP IPv6 on an interface. Use the **no** form of this command to remove the configuration.

mpls ipv6

no mpls ipv6

Parameter description

Parameter	Description
N/A	N/A

Defaults

LDP IPv6 is disabled on an interface by default.

Command mode

Interface configuration mode

Usage guidelines

Note

LDP IPv6 is allowed to be enabled only on an L3 interface.

Note

This command is not allowed to be configured on an interface bound with a uni-protocol VRF.

Note

If the interface is a tunnel interface, only the GRE tunnel can be enabled with LDP IPv6.

Caution

After LDP IPv6 function is enabled on an interface, the **label-switching** command must be configured to enable MPLS on the interface.

Examples

The following example enables LDP IPv6 on interface Gi4/1.

```
Ruijie(config)# interface Gi4/1
Ruijie(config-if)# mpls ipv6
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

mpls ip fragment

Use this command to set the processing an IP packet exceeds the MPLS MTU after this packet is encapsulated with the MPLS label.

mpls ip fragment

no mpls ip fragment

Parameter Description

Parameter	Description
N/A	N/A

Defaults

After the entered IP packet is encapsulated with the MPLS label, if the packet size exceeds the MPLS MTU, the original IP packet will be fragmented, encapsulated with the MPLS label, and then sent.

Command mode

Global configuration mode

Usage guidelines

This command is valid for only the process forward. In the case of hardware forward, a packet whose size exceeds the MTU is directly discarded. Use the no mpls ip fragment command to disable the fragment function for process forward. That is, if the size of an IP packet exceeds the MPLS MTU after this packet is encapsulated with the MPLS label, this packet will be directly discarded.

Examples

```
Ruijie(config)# no mpls ip fragment
```

Related commands

Command	Description
mpls ip	Enables MPLS globally.

Platform description

N/A

mpls ip icmp-error pop

Use this command to set the processing mode for ICMP error packets during the forwarding of MPLS packets.

mpls ip icmp-error pop *labels*

no mpls ip icmp-error pop

Parameter description

Parameter	Description
labels	Specifies the number of labels for packets to be processed.

Defaults

By default, the generated ICMP error packet continues to be forwarded along the original LSP

after being labeled with the original label stack.

Command mode Global configuration mode

Usage guidelines By default, the generated ICMP error packet continues to be forwarded along the original LSP after being labeled with the original label stack until it reaches the LSP egress. At the egress, the packet is rerouted and forwarded according to the inner IP address after its label stack is removed. You can use this command to change this default action by configuring packets with different numbers of labels to be processed differently. When the number of labels of a forwarded packet is less than or equal to the configured value, the ICMP error packet directly uses the IP route forwarding table of the FEC to which the top label corresponds.

Examples

```
Ruijie(config)# mpls ip icmp-error pop 2
```

Related commands

Command	Description
mpls ip	Enables MPLS globally.

Platform description N/A

mpls ip ttl propagate

Use this command to enable or disable the IP TTL copy function of the MPLS.
mpls ip ttl propagate {**public** | **vpn**}
no mpls ip ttl propagate {**public** | **vpn**}

Parameter description

Parameter	Description
public	Specifies whether to enable TTL copy function or not for the sent messages.
vpn	Specifies whether to enable TTL copy function or not for the forwarded messages.

Defaults The TTL copy function is enabled for both the sent and forwarded messages by default.

Command mode Global configuration mode

Usage guidelines The following are two modes of MPLS TTL:

- TTL copy mode: It is the default working mode. In this mode, the pushed label TTL is copied from the TTL of the existed header of the IP packet or the MPLS packet when the label is pushed. The TTL of the inner IP packet or the MPLS packet is copied from the TTL of the outer label when the label is popped.

- TTL non-copy mode: In this mode, set the value of pushed label TTL to 255 when Pushing the label and keep the value of the TTL of the inner IP packet or the MPLS packet when the label is popped.


Caution

After the TTL copy function is enabled, the TTL of the inner header is not copied but retained if it is smaller than the TTL of the outer header.

Examples The following example disables the TTL copy function of forwarded message:

```
Ruijie(config)# mpls ip ttl propagate public
```

Related commands

Command	Description
mpls ip	Enables MPLS globally.

Platform description N/A

mpls ldp distribution-mode

Use this command to set the label distribution mode used by LDP on each interface. Use the **no** form of this command to restore the default value.

mpls ldp distribution-mode {**dod | du**}

no mpls ldp distribution-mode

Parameter description

Parameter	Description
dod	Uses the downstream on-demand distribution mode.
du	Uses the downstream active distribution mode.

Defaults The downstream active distribution mode is used by default.

Command mode Interface configuration mode

Usage guidelines During the establishment negotiation of an LDP session, if two sides use different distribution modes, the DU mode will be used forcibly for both sides. This command does not affect LDP sessions that have been established on the interface.

Examples This example enables the LDP of the interface to work in DOD mode.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp distribution-mode dod
```

Related

Command	Description

commands	loop detection-mode	Configures loop detection.

Platform description N/A

mpls ldp hello-holdtime

Use this command to configure the holdtime in seconds for LDP Hello packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp hello-holdtime *seconds*
no mpls ldp hello-holdtime

Parameter description

Parameter	Description
seconds	Specifies the holdtime in seconds of Hello messages. The range is from 1 to 65535. Holdtime 65535 indicates that the Hello message will never time out.

Defaults The holdtime is set to 15 seconds by default.

Command mode Interface configuration mode

Usage guidelines This command is valid for only the LDP Link Hello packets for the basic discovery mechanism and may lead to a change in the interval for sending Hello messages. Use the **discovery targeted-Hello** command to set the Hello interval for the extended discovery mechanism.

Examples The following example sets the Link Hello holdtime of LDP on an interface to 30 seconds.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp Hello-holdtime 30
```

Related commands

Command	Description
mpls ldp hello-interval	Configures the interval for sending Hello messages.
discovery targeted-hello	Configures the interval and timeout time of sending Hello messages for the extended discovery mechanism.

Platform description N/A

mpls ldp hello-interval

Use this command to configure the holdtime in seconds for LDP Hello packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp Hello-interval *seconds*

no mpls ldp Hello-interval

Parameter description

Parameter	Description
seconds	Specifies the interval in seconds for sending Hello messages. The range is from 1 to 65535.

Defaults

The interval is set to 5 seconds by default.

Command mode

Interface configuration mode

Usage guidelines

The interval for sending Link Hello packets on an interface may not be consistent with that configured by this command.

- By default, if the minimum holdtime among all holdtimes negotiated with neighbors an interface is less than 15 seconds, the actually used interval for sending Hello packets is 1/3 of the minimum holdtime and the minimum interval is 1 second.
- By default, if the minimum holdtime among all holdtimes negotiated with neighbors of an interface is greater than or equal to 15 seconds, the actually used interval for sending Hello packets is 5 seconds.
- If the configured interval is greater than 1/3 of the minimum value among all holdtimes negotiated with neighbors of an interface, the actually used interval for sending Hello packets is 1/3 of the minimum holdtime and the minimum interval is 1 second.
- If the configured interval is less than 1/3 of the minimum value among all holdtimes negotiated with neighbors of an interface, the configured interval for sending Hello packets is used.

During configuration, this value must be less than the value of the Hello holdtime. This command is valid for only the LDP Link Hello packets for the basic discovery mechanism. Use the **discovery targeted-Hello** command to set the Hello holdtime for the extended discovery mechanism.

Examples

The following example sets the interval for sending Hello packets to 10 seconds.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp Hello-interval 10
```

Related commands

Command	Description
mpls ldp hello-holdtime	Configures the Hello packet holdtime in seconds.
discovery targeted-hello	Configures the interval and timeout time of sending Hello messages for the extended discovery mechanism.

Platform description	N/A

mpls ldp ignore nh-addr-check

Use this command to ignore the next-hop address check. Use the **no** form of this command to remove the configuration.

mpls ldp ignore nh-addr-check

no mpls ldp ignore nh-addr-check

Parameter description

Parameter	Description
N/A	N/A

Defaults Next hop address check is disabled by default.

Command mode config-mpls-router mode

Usage guidelines Run this command to ignore the next-hop address check and only match the outbound interface of the route.

This command is valid on a P2P interface.

If the peer end does not advertise the destination IP address of the P2P interface, run the [**no**] **mpls ldp ignore nh-addr-check** command and the LDP session will be reset on the corresponding interface.

Examples The following example ignores the next-hop address check.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface tunnel 1
Ruijie(config-if)#mpls ldp ignore nh-addr-check
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

mpls ldp keepalive-holdtime

Use this command to configure the holdtime for keepalive packets on each interface. Use the **no** form of this command to restore the default value.

mpls ldp keepalive-holdtime *seconds*

no mpls ldp keepalive-holdtime

Parameter description

Parameter	Description
seconds	Specifies the holdtime in seconds of keepalive packets. The range is from 15 to 65535.

Defaults The holdtime is set to 45 seconds by default.

Command mode Interface configuration mode

Usage guidelines This command is valid for the LDP sessions that are established after configuration of this command. It does not affect the LDP sessions that are established by the extended discovery mechanism. Use the targeted-session holdtime command to modify the keepalive holdtime of an LDP session that is established by the extended discovery mechanism.

Examples The following example sets the holdtime of the keepalive packet of LDP on an interface to 90 seconds.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp keepalive-holdtime 90
```

Related commands

Command	Description
targeted-session holdtime	Sets the holdtime of keepalive packets for the extended mechanism.

Platform description N/A

mpls ldp max-hop-count

Use this command to configure the maximum hop count allowed for loop detection on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-hop-count *number*

no mpls ldp max-hop-count

Parameter description

Parameter	Description
number	Specifies the maximum hop count allowed for loop detection. The range is from 1 to 255.

Defaults The default value is 254.

Command mode Interface configuration mode

Usage guidelines The value configured by this command is valid only after loop detection is configured. If the hop count value in the label mapping message or the label request message of LDP is greater than the configured value, it is deemed that a loop occurs. This command is valid for only the label mapping messages and label request messages that are received on the interface after the configuration of this command.

Examples The following example sets the LDP hop count of the interface to 30.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp max-hop-count 30
```

Related commands

Command	Description
loop-detection	Configures LDP loop detection.

Platform description N/A

mpls ldp max-label-requests

Use this command to configure the maximum number of label requests allowed on each interface. Use the **no** form of this command to restore the default value.

mpls ldp max-label-requests *times*

no mpls ldp max-label-requests

Parameter description

Parameter	Description
times	Specifies the maximum number of requests. The range is from 0 to 255.

Defaults There is no limit by default, indicating that label requests are retransmitted until a label mapping message is received.

Command mode Interface configuration mode

Usage guidelines This command is valid for only LDP sessions that are established after configuration of this command. The value 0 means that the label request will not be retransmitted.

Examples The following example sets the maximum number of label requests of LDP allowed on an interface to 5.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp max-label-requests 5
```

Related commands

Command	Description
mpls ldp distribution-mode	Configures the label distribution mode.

Platform description N/A

mpls ldp max-path-vector

Use this command to configure the maximum path vector value allowed for loop detection on each interface. Use the **no** form of this command to restore the default value.
mpls ldp max-path-vector *number*
no mpls ldp max-path-vector

Parameter description

Parameter	Description
number	Specifies the maximum path vector value. The range is from 0 to 255.

Defaults The default value is 254.

Command mode Interface configuration mode

Usage guidelines The configured path vector value takes effect only after the LDP instance enables loop detection. If the number of LDR IDs contained in the path vector list of the label mapping message or the label request message of LDP is greater than the configured maximum path sector value, it is deemed that a loop occurs. This command is valid for only LDP sessions that are established after configuration of this command.

Examples The following example sets the maximum path vector value of LDP on an interface to 10.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp max-path-vector 10
```

Related commands

Command	Description
loop-detection	Sets LDP loop detection.

Platform description N/A

mpls ldp max-pdu

Use this command to configure the maximum PDU. Use the **no** form of this command to restore the default value.

mpls ldp max-pdu *max-pdu*

no mpls ldp max-pdu

Parameter description

Parameter	Description
max-pdu	Specifies the maximum PDU (in bytes) used for LDP message exchange in exchanging the LDP messages. The range is from 256 to 4096.

Defaults The default value is 4096.

Command mode Interface configuration mode

Usage guidelines This command is valid for only LDP sessions that are established on the interface after configuration of this command.

Examples The following example sets the maximum length of LDP messages to 256.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)# mpls ldp max-pdu 256
```

Platform description N/A

mpls ldp priority

Use this command to set the LDP priority on the interface. Use the **no** form of this command to remove the configuration.

mpls ldp priority *priority-value*

no mpls ldp priority

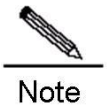
Parameter description

Parameter	Description
priority-value	Sets the LDP priority value in the range from 256 to 768. The lower the value, the higher the priority.

Defaults The default priority value is 512.

Command mode Interface confgiuration mode

Usage guidelines



Run this command to change the LDP interface priority.

If equal-cost routes are available, the LDP will select the outbound interface with the highest priority to establish an LSP.

If equal-cost routes have the same priority, the LDP will select one randomly.

Examples The following example sets the LDP priority value to 300.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface GigabitEthernet0/0
Ruijie(config-if)#mpls ldp priority 300
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

mpls ldp transport-address

Use this command to set the transport address used by basic LDP sessions on the interface. Use the **no** form of this command to restore the default value.

mpls ldp transport-address {interface | *ip-address***}**

no mpls ldp transport-address

Parameter description

Parameter	Description
interface	Indicates that the LDP session uses the main address of an interface itself.
ip-address	Indicates that the LDP session uses an IP address specified by this parameter.

Defaults The LSR ID of LDP is used as the transport address by default.

Command mode Interface configuration mode

Usage guidelines

This command is valid for only LDP sessions that are established by basic discovery mechanism, instead of the extended discovery mechanism. When this interface transport address is configured, this command is valid for only LDP sessions that are established by basic discovery mechanism after configuration of this command.

Examples

The following example sets the transport address to the main address of the interface that is used for establishing basic LDP sessions.

```
Ruijie(config)# interface vlan 10
Ruijie(config-if)#mpls ldp transport-address interface
```

Related commands

Command	Description
show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.
transport-address	Globally configures the transport address used by basic LDP sessions.

Platform description

N/A

mpls mtu

Use this command to configure the MPLS MTU. Use the **no** form of this command to restore the default value.

mpls mtu *mtu*

no mpls mtu

Parameter description

Parameter	Description
mtu	Specifies the length (in bytes) of a label packet supported by the interface. The range is from 64 to 1500.

Defaults

The MPLS MTU is equal to the interface MTU by default.

Command mode

Interface configuration mode

Usage guidelines

The MTU of an MPLS label packet that can be transmitted on an interface is equal to the interface MTU by default. The MPLS MTU determines whether an MPLS packet needs to be fragmented when being transmitted. The MPLS MTU is the total length of the MPLS encapsulating and encapsulated (IP) layers. The MPLS MTU on the interface cannot exceed the actual transmission capability of the interface.

This command is valid for only process forwarding and router fast forwarding instead of switches that use ASIC forwarding. The switch forwards packets according to the actually configured MTU on the interface and discards packets that exceed the configured MTU. You can use the mtu

command in interface configuration mode to adjust the MTU on the interface.
During configuration, it is recommended that the MTU be adjusted to prevent deterioration of the forwarding performance due to fragmentation.

Examples

```
Ruijie(config)# interface Gi4/1
Ruijie(config-if)# mpls mtu 1510
```

Related commands

Command	Description
mpls ip	Enables the MPLS in global configuration mode.

Platform description

N/A

mpls router ldp

Use this command to enable LDP. Use the **no** form of this command to disable LDP.
mpls router ldp [*vrf-name*]
no mpls router ldp [*vrf-name***]**

Parameter description

Parameter	Description
vrf-name	Indicates whether LDP of a VRF is enabled or disabled.

Defaults

LDP is disabled by default.

Command mode

Global configuration mode

Usage guidelines

The number of LDP instances is limited by the number of VRFs on a device. Each VRF can start one LDP instance. If no VRF is specified, LDP of all VRFs is enabled or disabled by default.

Examples

1) The following example enables LDP of all VRFs and enters LDP configuration mode.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# ldp router-id interface vlan 10 force
The following example enables LDP of vpna and enters LDP configuration mode.
Ruijie(config)# mpls router ldp vpna
Ruijie(config-mpls-router)# ldp router-id interface vlan 10 force
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

mpls static ftn

Use this command to add one FTN entry to the global FTN table. Use the **no** form of this command to delete a specified FTN entry from the FTN table.

mpls static ftn *ip-address/mask* **out-label** *label* **nexthop** *interface-name nexthop-ip*

no mpls static ftn *ip-address//mask*

Parameter description

Parameter	Description
ip-address//mask	Specifies the FEC, namely the destination address.
out-label *label*	Specifies the out label of this FEC.
nexthop *interface-name nexthop-ip*	Specifies the next hop of this FEC, including the egress and the IP address of the next hop.

Defaults N/A

Command mode Global configuration mode

Usage guidelines This command adds an FTN entry to the global FTN table. After a MPLS-enabled router receives an IP packet, it looks up for the next hop in the FTN table according to the destination address of the IP packet by using the maximum match method. If the next hop is found, the router performs label forwarding on the IP packet. For the FTN whose destination address and mask are both 0, this command is valid only when this default route exists in the IP route forwarding table.

Examples

```
Ruijie(config)# mpls static ftn 192.168.0.0/16 out-label 100 nexthop gi4/1 10.10.10.1
```

Related commands

Command	Description
show mpls forwarding-table	Shows the brief information about the global FTN table.

Platform description N/A

mpls static ilm in-label

Use this command to add an ILM entry to the ILM table. Use the **no** form of this command to delete the configured ILM entry.

mpls static ilm in-label *in_label* **forward-action swap-label** *label* **nexthop** *interface-name nexthop-ip* **fec** *ip-address/mask*

mpls static ilm in-label *in_label* **forward-action pop-l3vpn-nexthop** *vrf-name* **nexthop**

interface-name nexthop-ip **fec** *ip-address/mask*

mpls static ilm in-label *in_label* **forward-action pop-l2vc-destport** *vc_id vc-peer-addr*

no mpls static ilm in-label *in_label*

Parameter description

Parameter	Description
In_label	Specifies the in label value of the ILM entry.
forward-action	Specifies the forward behavior of the ILM entry. **swap-label:** ILM entry used for the public network, indicating that the label is switched and forwarded. **pop-l3vpn-nexthop:** ILM entry used for the L3 VPN, indicating that the label is popped and the packet is forwarded to the next hop of the specified VRF. **pop-l2vc-destport:** ILM entry used for the L2 VPN, indicating that the label is popped and the packet is forwarded from the specified interface.
label	Specifies the out label value of the switched label value if the forward behavior is **swap-label**.
vrf-name	Specifies the VPN of the ILM (that is, the VRF) if the forward behavior is **pop-l3vpn-nexthop**.
Interface-name	Specifies the forward egress if the forward behavior is **pop-l2vc-destport**.
nexthop *interface-name nexthop-ip*	Specifies the next hop, including the egress and the IP address of the next hop.
fec	Specifies the FEC for which the ILM is created.
ip-address/mask	Specifies a destination network. It corresponds to the FEC format of the global or L3 VPN application.
vc_id	Specifies a VC instance. It corresponds to the FEC format of the L2 VPN application.
vc-peer-addr	Specifies the address of the VC peer.

Defaults N/A

Command mode Global configuration mode

Usage guidelines This command adds an ILM entry to the ILM table. After the MPLS-enabled router receives an IP packet that contains the label, it looks up for the next hop in the ILM table according to the label of the IP packet by using the maximum match method. If the next hop is found, it carries out forward

actions on the IP packet, such as switching and popping the label of the IP packet.

Examples

```
Ruijie(config)# mpls static ilm in_label 20 forward-action swap-label 30
nexthop gi4/2 10.10.10.1 fec 172.16.0.0/26
```

Related commands

Command	Description
show mpls forwarding-table	Shows the information about the MPLS forwarding table.

Platform description

N/A

mpls static l2vc-ftn

Use this command to configure a static VC FTN entry. Use the **no** form of this command to delete the configured FTN entry.

mpls static l2vc-ftn *vc_id vc_peer_ip* **out_label** *label*

no mpls static l2vc-ftn *vc_id vc_peer_ip*

Parameter description

Parameter	Description
vc_id	Specifies the ID of the VC instance.
vc_peer_ip	Specifies the IP address of the peer PE of the VC.
out_label *label*	Specifies the out label used for forwarding of the VC FTN.

Defaults

N/A

Command mode

Global configuration mode

Usage guidelines

This command creates an FTN entry for the VC instance. After the router receives a frame from the AC that is bound with this VC, the frame is added with the private network label according to the content of this FTN entry. In addition, the router finds the LSP to the peer PE according to the IP address of the peer PE of the VC, and then forwards the frame.

Examples

```
Ruijie(config)# mpls static l2vc-ftn 1 10.10.10.1 out_label 21
```

Related commands

Command	Description
show mpls l2vc ftn_table	Shows FTN entries of all VC instances.
show mpls forwarding-table	Shows forwarding entries of the MPLS.

Platform description N/A

mpls static l3vpn-ftn

Use this command to add an FTN entry of one L3 VPN. Use the **no** form of this command to delete this FTN entry.

mpls static l3vpn-ftn *vrf-name ip-address/mask* **out-label** *label* **remote-pe** *ip-addr*
mpls static l3vpn-ftn *vrf-name ip-address/mask* **local-forward nexthop** *interface-name nexthop-ip*
no mpls static l3vpn-ftn *vrf ip-address/mask*

Parameter description

Parameter	Description
vrf-name	Specifies the VRF. The FTN entry will be added to the FTN table of this VRF.
ip-address/mask	Specifies the FEC, that is, the destination network.
out-label *label*	Indicates that the corresponding private network FTN will reach the peer PE through the LSP tunnel. This parameter also specifies the out label used for forwarding.
remote-pe *ip-addr*	Specifies the address of the egress PE.
local-forward nexthop *interface-name nexthop-ip*	Indicates that the corresponding private network FTN will be directly forwarded to the next hop by the local PE. This parameter also specifies the egress and IP address of the next hop.

Command mode Global configuration mode

Usage guidelines This command adds an FTN entry to the FTN table of the specified VRF. After the MPLS-enabled router receives an IP packet, it looks up for the next hop in the FTN table according to the destination address of the IP packet by using the maximum match method. If the next hop is found, it performs label forwarding on the IP packet. For the FTN whose destination and mask is 0, it is valid only when this route exists in the IP route forwarding table.

Examples

```
Ruijie(config)# mpls static l3vpn-ftn 192.168.0.0/16 out-label 100 remote-pe 10.10.10.1
```

Related commands

Command	Description
show mpls forwarding-table	Shows the brief information about the global FTN table.

Platform N/A

description

neighbor

Use this command to create an LDP extended peer. Use the **no** form of this command to delete the LDP extended peer.
neighbor *ip-address*
no neighbor *ip-address*

Parameter description

Parameter	Description
ip-address	Specifies the router ID of the peer LSR.

Defaults The LDP extended peer is not configured by default.

Command mode **config-mpls-router mode**

Usage guidelines To establish an extended LDP session, the LDP extended peer must be configured on the LSRs on both ends of the extended LDP session. If the extended peer is configured on only one LSR, the extended LDP session cannot be established.

Examples The following example configures 10.10.10.1 as an extended peer of the LSR.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# neighbor 10.10.10.1
```

Related commands

Command	Description
show mpls ldp discovery	Shows the information about neighbors discovered by the LDP.
show mpls ldp neighbor	Shows the LDP session state.

Platform description N/A

neighbor labels accept

Use this command to configure an ACL rule based on which the LSR filters label mapping messages for the LDP peer. Use the **no** form of this command to delete the ACL rule.
neighbor *ip-address* **labels accept** *acl-name*
no neighbor *ip-address* **labels accept**

Parameter description

Parameter	Description
ip-address	Specifies the router ID of the peer LSR.

acl-name	Specifies the name of the ACL rule.

Defaults The filtering rule is not configured by default.

Command mode config-mpls-router mode

Usage guidelines This command is valid for only the IP route FEC instead of other FECs (such as the PW FEC). Assume that this command is used to configure a rule for filtering the in label mapping messages. If the neighbor is specified, only label mapping messages of the FEC that meet the ACL rule can be received and other label mapping messages sent by this neighbor are discarded. Label mapping messages sent by other neighbors, however, are not affected and are still received. If this command is configured for a specified neighbor but no filtering rule is configured for the corresponding ACL, label mapping messages of all FECs sent by this neighbor are discarded. When the rule is cancelled by using the no form of this command, label mapping messages that have been filtered are not affected (that is, messages that have been discarded cannot be recovered) and only label mapping messages received thereafter are affected. In this case, the clear mpls ldp neighbor command must be used to reset the LDP session. Only one rule can be configured for one neighbor. If rules are configured repeatedly, the rule that is configured later overwrites the rule that is configured earlier. Each LDP instance can be used to configure filtering rules for a maximum of 64 neighbors.

Examples The following example enables the router to receive only label mapping messages of the FEC with 192.168.0.0/16 as the route prefix and sent from the neighbor 10.10.10.1, and discard those of other FECs sent from this neighbor.

```
Ruijie(config) #ip access-list standard fec_acl
Ruijie(config-std-nacl)#permit 192.168.0.0 0.0.255.255
Ruijie(config-std-nacl)# exit
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# neighbor 10.10.10.1 labels accept fec_acl
```

Related commands

Command	Description
clear mpls ldp neighbor	Forcibly disconnects an LDP session.
show mpls ldp neighbor	Shows the LDP session state.

Platform description N/A

neighbor password

Use this command to enable MD5 authentication of LDP. Use the **no** form of this command to disable MD5 authentication of LDP.

neighbor *ip-address* **password [0 | 7]** *pwd-string*

no neighbor *ip-address* **password**

Parameter description

Parameter	Description
ip-address	Specifies the transport address of the peer LSR.
[0 | 7]	(Optional) 0 means that the key is entered in plain text and 7 means that the key is entered in encrypted text. The key is entered in plain text by default.
pwd-string	Specifies the password string, which is case-sensitive. If the password string is entered in plain text, it is a string of 1 to 25 characters; if the password string is entered in encrypted text, it is a string of 1 to 52 characters.

Defaults

MD5 authentication of LDP is disabled by default.

Command mode

config-mpls-router mode

Usage guidelines

A key can be entered in either plain text or encrypted text. In the former case, if the **service password-encryption** command is used to enable the encryption service in global configuration mode, the key is saved in encrypted text when the current configuration is saved or viewed.

To enable LDP authentication function, the keys configured on both ends of the LDP peer must be the same. Any change to the key will cause disconnection of established LDP sessions and an attempt to re-establish them.

- If a router that plays the active role is configured with a key but the router that plays the passive role is not configured with a key, the router that plays the passive role sends the following message when an attempt is made to establish a session between two routers:

```
%TCP-6-BADAUTH_MD5_UNEXPECTED: Found unexpected MD5 option from (%d.%d.%d.%d, %d) to (%d.%d.%d.%d, %d)
```

- If a router that plays the active role is not configured with a key but the router that plays the passive role is configured with a key, the router that plays the passive role sends the following message when an attempt is made to establish a session between two routers:

```
%TCP-6-BADAUTH_MD5_NOT_FOUND: Unable to find expected MD5 option from (%d.%d.%d.%d, %d) to (%d.%d.%d.%d, %d)
```

- If the keys configured on two routers are not the same, the router that plays the passive role sends the following message when an attempt is made to establish a session between two routers:

```
%TCP-6-BADAUTH_MD5_INVALID: Failed to detect MD5 option from (%d.%d.%d.%d, %d) to (%d.%d.%d.%d, %d)
```

Examples

The following example enables MD5 authentication for sessions between the router and 10.10.10.1 and sets the plain text key to 123456.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# neighbor 10.10.10.1 password 123456
```

Related commands

Command	Description
show mpls ldp discovery	Shows the information about neighbors discovered by LDP.
show mpls ldp neighbor	Shows the LDP session state.
neighbor *ip-address*	Creates an LDP extended peer.

Platform description

N/A

neighbor valid-hops

Use this command to set the number of GTSM protection hops for an LDP session. Use the **no** form of this command to remove the configuration.

neighbor *ip-address* **valid-hops** { *hops* | **unlimited** }

no neighbor *ip-address* **valid-hops**

Parameter description

Parameter	Description
ip-address	Configures the router ID of the LSR.
hops	Specifies the number of GTSM protection hops, in the range from 1 to 255.
unlimited	Unlimits the number of GTSM protection hops.

Defaults

The number of GTSM protection hops is not limited by default.

Command mode

config-mpls-router mode

Usage guidelines

Examples

The following example sets the number of GTSM protection hops to 4.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# neighbor 10.10.10.1 valid-hops 4
```

Related commands

Command	Description
N/A	N/A

Platform description

N/Al

ping mpls

Use this command to test the connectivity of an MPLS LSP.

ping mpls ipv4 *ip-address/mask* [**repeat** *repeat*] [**ttl** *time-to-live*] [**timeout** *timeout*] [**size** *size*] [**interval** *mseconds*] [**source** *ip-address*] [**destination** *ip-address*] [**force-explicit-null**] [**pad** *pattern*] [**reply mode** {**ipv4** | **router-alert**}] [**dsmap**] [**flags fec**] [**verbose**]

Parameter description

Parameter	Description
ip-address/mask	Specifies the IPv4 address and subnet mask length of the destination FEC to be tested.
repeat *repeat*	(Optional) Specifies the number of times an Echo Request packet is retransmitted. The range is from 1 to 2147483647. The default value is 5.
ttl *time-to-live*	(Optional) Specifies the initial MPLS TTL value for sending packets. The range is from 1 to 255. The default value is 255.
timeout *timeout*	(Optional) Specifies the timeout time for a packet. The range is from 0 to 3600. The default value is 2.
size *size*	(Optional) Specifies the size of a packet. The range is from 84 to 18024. The default value is 84.
interval *mseconds*	(Optional) Specifies the minimum interval time (in milliseconds) between two Echo Request packets that are sent consecutively. The range is from 0 to 3600000. The default value is 0.
source *ip-address*	(Optional) Specifies the source address. It is the destination address when the peer sends an Echo Reply packet.
destination *ip-address*	(Optional) Specifies the 127/8 segment address. It is used to pad the IP header. The default value is 127.0.0.1.
force-explicit-null	(Optional) Indicates whether an explicit null label is forcibly added to the MPLS label. An explicit null label is not forcibly added to the MPLS label by default.
pad *pattern*	(Optional) Specifies the pad pattern of a packet. 0xABCD is padded by default.
reply mode {ipv4 | router-alert}	(Optional) Specifies the reply mode of the Echo Request packet: **ipv4**: Reply with an IPv4 UDP packet. It is the default value. **router-alert**: Reply with an IPv4 UDP packet with the Router Alert option.
dsmap	(Optional) Indicates that downstream information must be returned.
flags fec	(Optional) Enables the forcible FEC stack check.
verbose	(Optional) Shows detailed information about Echo Reply packets. The information is not shown by default.

Defaults See the preceding parameter description.

Command mode Privileged mode

Usage guidelines You can change some default parameter values by specifying optional parameters. You can either directly type this command or enter the interactive typing mode by pressing Enter after typing the **ping mpls** command.

Examples

1) The following example tests the connectivity from the local device to the LSP of 10.10.10.10/32.

```
Ruijie# ping mpls ipv4 10.10.10.10/32 verbose
Sending 5, 84-byte MPLS Echoes to 10.10.10.10/32,
   timeout is 2 seconds, send interval is 0 msec:
      < press Ctrl+C to break >
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
 'L'-labeled output interface,'B'-unlabeled output interface,
 'D'-DS Map mismatch,'F'-no FEC mapping,'f'-FEC mismatch,
 'M'-malformed request,'m'-unsupported tlvs,'N'-no label entry,
 'P'-no rx intf label prot,'p'-premature termination of LSP,
 'R'-transit router,'I'-unknown upstream index,
 'X'-unknown return code,'x'-return code 0
Type escape sequence to abort.
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
!   size 84, reply addr 192.168.201.208, return code 3
Success rate is 100 percent(5/5),round-trip min/avg/max=20/36/60 ms
```

2) The following example returns the downstream information. In this case, use the **dsmap** and **ttl** parameters together because the downstream information is not returned if it reaches the egress LSR.

```
Ruijie# ping mpls ipv4 10.40.10.10/32 dsmap ttl 1
Sending 5, 84-byte MPLS Echoes to 10.4(2)0.10.10/32,
    timeout is 2 seconds, send interval is 0 msec:
       < press Ctrl+C to break >
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
 'L'-labeled output interface,'B'-unlabeled output interface,
 'D'-DS Map mismatch,'F'-no FEC mapping,'f'-FEC mismatch,
 'M'-malformed request,'m'-unsupported tlvs,'N'-no label entry,
 'P'-no rx intf label prot,'p'-premature termination of LSP,
 'R'-transit router,'I'-unknown upstream index,
 'X'-unknown return code,'x'-return code 0
Type escape sequence to abort.
L
```

```
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
L
Echo Reply received from 192.168.201.208
  DSMAP 0,DS Router Addr 192.168.198.2,DS Intf Addr 192.168.198.2
    Depth Limit 0, MRU 1508 [Labels: implicit-null Exp: 0]
Success rate is 0 percent (0/5)
```

Field	Description
!	A correct Reply packet is received, indicating that the LSP is connected.
Q	The Request packet is not sent, indicating that there is no LSP corresponding to the destination FEC on the local device.
.	The Reply packet times out, indicating that no Reply packet is received within a specified period of time.
L	There is an out label corresponding to the FEC on the router that returns a Reply packet, indicating that the router that returns a Reply packet is an intermediate router of the LSP.
B	There is no out label corresponding to the FEC on the router that returns a Reply packet, indicating that the LSP is interrupted.
D	Authentication information carried in Downstream Mapping TLV does not match the information on the router that returns a Reply packet.
F	There is no FEC mapping carried in the corresponding TargetFec on the router that returns a Reply packet.
f	The label of the current label stack in the router that returns a Reply packet is inconsistent with the label of FEC mapping carried in TargetFec.
M	The format of the Request packet received by the router that returns a Reply packet is incorrect.
m	The Request packet received by the router that returns a Reply packet has TLVs that are not supported.
N	The router that returns a Reply packet does not have an instance corresponding to the in label, indicating that the labels are not synchronous.

P	The protocol for transmitting packets in the router that returns a Reply packet is inconsistent with that recorded in TargetFec stack.
p	Packet transmission is terminated prematurely.
R	The reserved value is returned.
I	The upstream interface index is unknown.
X	The return value is unknown.
x	The return value is 0.

Related commands

Command	Description
traceroute mpls	Views the LSRs on the MPLS LSP.

Platform description N/A

propagate-release

Use this command to enable the label release propagation function. Use the **no** form of this command to disable this function so that no label release messages are propagated.

propagate-release

no propagate-release

Parameter Description

Parameter	Description
N/A	N/A

Defaults The label release propagation function is disabled by default.

Command mode config-mpls-router mode

Usage guidelines This command is valid for only the label release messages that are received from the LDP instance after configuration of this command.

Examples The following example enables the label release propagation function of the LDP instance.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# propagate-release
```

Related commands

Command	Description
show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.

Platform description N/A

route wait label-mapping

Use this command to set the time to wait for label mapping. Use the **no** form of this command to remove the configuration.

route wait label-mapping *seconds*

no route wait label-mapping

Parameter description

Parameter	Description
seconds	Sets the time to wait for lable mapping, in the range from 0 to 65535 seconds.

Defaults The default waiting time is 120 seconds.

Command mode Global configuration mode

Usage guidelines The LDP may delete the old LSP corresponding to the next hop when the new LSP is not established. In this case, the traffic is terminated until the new LSP is established. After this command is configured, the LDP will delete the old LSP after a period. During this period, if the new LSP is established, traffic will be switched over the new LSP immediately. If the period times out and the new LSP is not established, the old LSP will be deleted

Examples The following example sets the time to wait for label mapping to 100 seconds.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)#route wait label-mapping 100
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

session protection

Use this command to enable LDP session protection. Use the **no** form of this command to remove the configuration.

session protection [**for acl** *acl_name*] [**duration** { **infinite** | *seconds* }]

no session protection [**for acl**] [**duration**]

Parameter

Parameter	Description

description

-	Enables/Disables LDP session protection.
for acl *acl_name*	(Optional) Specifies an ACL list.
duration	(Optional) Configures the protection time. During this time, LDP session is protected and will not be down.
infinite	After session protection is enabled, LDP session will not be down.
seconds	Configures the protection time, in the range from 30 to 2147483 seconds.

Defaults

LDP session protection is disabled.
No ACL is specified by default.
The default protection time is 86400 seconds.

Command mode

config-mpls-router mode

Usage guidelines

Examples

The following example enables LDP session protection.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# session protection
```

The following example enables LDP session protection for VRF instance vpna.

```
Ruijie(config)# mpls router ldp vpna
Ruijie(config-mpls-router)# session protection
```

The following example enables LDP session protection for LSR 10.10.10.10.

```
Ruijie(config)# ip access-list standard acl_1
Ruijie(config-std-nacl)# permit host 10.10.10.10
Ruijie(config-std-nacl)# exit
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# session protection for acl acl_1
```

The following example disables LDP protection for ACL_1.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# no session protection for acl acl_1
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

show ip ref mpls forwarding-table

Use this command to show MPLS express forwarding information.

show ip ref mpls forwarding-table [**vrf** *vrf-name*] {**ftn** [*ip-address*/*mask*] | **ilm** [*label*]} [**frr**] [**detail**]

Parameter description

Parameter	Description
vrf *vrf-name*	Shows the specified VRF entry information.
ftn [*ip-address/mask*]	Shows FTN entry information.
ilm [*label*]	Shows ILM entry information.
frr	Shows FRR entry information when and only when there are active/standby FTN/ILM entries.
detail	Shows detailed information about FTN/ILM entries.

Defaults

N/A

Command mode

Privileged mode

Usage guidelines

If a VRF is not specified in this command, it indicates that FTN/ILM entry information of all VRFs is displayed.

Examples

1) The following example shows FTN entry information of all VRFs.

```
Ruijie#show ip ref mpls forwarding-table ftn
Label Operation Code:
PH--PUSH label
IP--IP lookup forward
FEC      VRF  Out Label  OP  Out IF  Adj    Nexthop
1.1.1.1/32   0    1024    PH   2      7    20.0.0.6
2.2.2.2/32   0    1026    PH   4      3    21.1.1.1
```

FEC: In the case of FTN for IP routes, the IP address and mask are displayed for the FEC field; in the case of FTN for L3 VPN, "--" is displayed for the FEC field.

VRF: Indicates the VRF to which the FTN belongs.

Out Label: Indicates an out label.

OP: Indicates an operation behavior that a packet hits the forwarding entry. This behavior includes the following:

Field	Description
PH	Indicates that an IP packet needs to be added with labels (perhaps one to three labels) and then forwarded to the next hop after hitting the entry. If imp-null is displayed as the out label, the imp-null label is not added in the actual forwarding process.

IP	Indicates an IP packet needs to be forwarded across VRFs after hitting the entry. This type of entry is the forwarding entry across VRFs of one VPN.

Out IF: Indicates the outgoing interface for packet forwarding, using the interface index number.

Adj: Indicates the adjacency identifier.

Nexthop: Indicates the next hop for packet forwarding. "--" is displayed for a forwarding entry with an ineffective next hop address.

2) The following example shows FRR information for FTN entries under all VRFs.

```
Ruijie#show ip ref mpls forwarding-table ftn frr
Label Operation Code:
PH--PUSH label
IP--IP lookup forward
Status codes: m – main entry, b – backup entry, * – active
FEC       VRF    Out Label  OP  Out IF  Adj    Nexthop
m*1.1.1.1/32   0     1024     PH  2       7      20.0.0.6
b 1.1.1.1/32   0     1025     PH  3       2      20.0.1.6
The following example shows ILM entry information of all VRFs.
Ruijie#show ip ref mpls forwarding-table ilm
Label Operation Code:
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
PN--POP label and forward to nexthop
PI--POP label and do ip lookup forward
PC--POP label and continue lookup(IP or Label)
DP--DROP packet
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
In Label     Out Label  OP  VRF    Out IF  Adj    Nexthop
1024         1028     SW  0        2      7     20.0.0.6
1025         1029     SW  0        3      2     20.0.1.6
```

In Label: Indicates an in label.

Out Label: Indicates an out label.

OP: Indicates an operation behavior that a packet hits the forwarding entry. This behavior includes the following:

Field	Description
PP	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry, that is, perform forwarding of the last but one hop.
SW	Indicates that an MPLS packet needs to exchange labels and be forwarded to the next hop directly after hitting the entry.
SP	Indicates that an MPLS packet needs to exchange top labels, added with a label, and be forwarded to the next hop after hitting the entry. Exchanged labels are displayed for the out label field, and one to two labels may be added.
PN	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry.

PI	Indicates that an MPLS packet needs to remove all labels and be forwarded according to the destination IP address after hitting the entry.
PC	Indicates that an MPLS packet removes the top label and is forwarded according to the query result in the label forwarding table after hitting the entry. In the case of an IP packet, it is forwarded according to the destination IP address.
PM	Indicates that an MPLS packet needs to remove the label and is forwarded according to the destination MAC of the inner packet (VPLS application) after hitting the entry.
PV	Indicates that an MPLS packet needs to remove the label and is forwarded from a specified egress (VPWS application) after hitting the entry.
DP	Indicates that a packet is discarded after hitting the entry.

VRF: Indicates the VRF to which the ILM belongs.

Out IF: Indicates the outgoing interface for packet forwarding, using the interface index number.

Adj: Indicates the adjacency identifier.

Nexthop: Indicates the next hop for packet forwarding. "--" is displayed for a forwarding entry with an ineffective next hop address.

1. The following example shows FRR information for ILM entries under all VRFs.

```
Ruijie#show ip ref mpls forwarding-table ilm frr
Label Operation Code:
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
PN--POP label and forward to nexthop
PI--POP label and do ip lookup forward
PC--POP label and continue lookup(IP or Label)
DP--DROP packet
Status codes: m - main entry, b - backup entry, * - active
In Label    Out Label  OP  VRF    Out IF  Adj    Nexthop
m*1024        1028      SW   0       2     7    20.0.0.6
b 1024        1029      SW   0       3     2    20.0.1.6
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

show mpls forwarding-table

Use this command to show the MPLS forwarding table.

show mpls forwarding-table [*ip-address/mask*] [**label** *label*] [**interface** *interface-name*] [**next-hop** ***i****p-address*] [**ftn** [**ip** | **vc**]] [**ilm** [**ip** | **vc**]] [{**vrf** *vrf-name* | **global**} [**ftn** | **ilm**]] [**detail** | **summary**]

Parameter

Parameter	Description

description

ip-address/mask	Shows ILM and FTN entries of a specified FEC.
label *label*	Shows the ILM entry of a specified label.
interface *interface-name*	Shows the MPLS forwarding entry (ILM and FTN) of a specified egress.
next-hop *ip-address*	Shows the MPLS forwarding entry (ILM and FTN) of a specified next-hop address.
ftn	Shows an FEC mapping entry.
ilm	Shows a label forwarding entry.
ip	Shows the MPLS forwarding entry of an IP application (including unicast route and L3 VPN).
vc	Shows the MPLS forwarding entry added by the VC.
vrf *vrf-name*	Shows the MPLS forwarding entry related to a VRF.
detail	Shows the detailed information about the MPLS forwarding entry.
global	Shows global non-VRF MPLS forwarding entries, excluding FTN and ILM entries of the VC.
summary	Shows the statistics information of MPLS process forwarding.

Defaults

No parameter is specified in this command by default, indicating that all MPLS forwarding entries are displayed.

Command mode

Privileged mode

Usage guidelines

Use the **show mpls forwarding-table** command to show information about all MPLS forwarding entries (including ILM and FTN entries).

Use the **show mpls forwarding-table** *ip-address/mask* command to show information about specified MPLS forwarding entries (including ILM and FTN entries).

Use the **show mpls forwarding-table label** *label* command to show the ILM forwarding entries of a specified label.

Use the **show mpls forwarding-table interface** *interface-name* command to show the MPLS forwarding entries of a specified egress (including FTN and ILM entries).

Use the **show mpls forwarding-table next-hop** *ip-address* command to show the MPLS forwarding entries of a specified next hop (including FTN and ILM entries).

Use the **show mpls forwarding-table detail** command to show detailed information about all MPLS forwarding entries (including ILM and FTN entries).

Use the **show mpls forwarding-table vrf** command to show all MPLS forwarding entries (including ILM and FTN entries) which belong to a VRF.

Use the **show mpls forwarding-table vrf** *vrf-name* **ftn** command to show information about all FTN entries which belong to a VRF.

Use the **show mpls forwarding-table vrf** *vrf-name* **ilm** command to show information about all ILM entries which belong to a VRF.

Use the **show mpls forwarding-table ftn ip** command to show FTN entries of unicast routes and L3 VPN application.

Use the **show mpls forwarding-table ilm ip** command to show ILM entries of unicast routes and L3 VPN application.

Use the **show mpls forwarding-table ftn** command to show all FTN entries.

Use the **show mpls forwarding-table ilm** command to show all ILM entries.

Use the **show mpls forwarding-table ftn vc** command to show all FTN entries of L2 VPN.

Use the **show mpls forwarding-table ilm vc** command to show all ILM entries of L2 VPN.

Use the **show mpls forwarding-table ftn detail** command to show detailed information about all FTN entries.

Use the **show mpls forwarding-table ilm detail** command to show detailed information about all ILM entries.

Examples

1) The following example shows all MPLS forwarding entries.

```
Ruijie#show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP—-SWAP topmost label and push new label
DP—-DROP packet
PC—-POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
Local Outgoing OP FEC        Outgoing      Nexthop
laebl label                   interface
--    1025      PH 119.1.1.0/24(V)  Gi3/19    10.0.10.1
--    1026      PH 120.1.1.0/24     Gi3/18      10.0.2.1
--    imp-null   PH 130.1.1.0/24    Gi3/18      10.0.2.1
1025   1027      SP 100.1.1.0/24     Vl8          192.1.2.1
1026   1028      SW 120.1.2.0/24     Gi3/19       10.0.2.1
1027   imp-null   PP 121.1.1.0/24     Fa3/1        11.0.0.1
--    --         IP 167.168.195.0/24 Fa3/2        120.1.1.1
1028   --         PC 167.168.196.0/24 --           --
1029   --         PN 167.168.197.0/24(V) Vl4       1.0.0.1
1030   --         PI VRF(vpna)         --          --
1031   --         PV VC(20,1.1.1.1)    Vl5          --
--    1029       PH VC(20,1.1.1.1)    Vl10         192.1.2.1
1032   --         PI 192.1.1.0/24(V)  Vl101        172.2.1.2
1033   1030       SW 193.1.1.0/24(V)  Vl102        10.2.1.2
```

Local label: It is the label distributed by the FEC to other devices, namely the in label of an ILM

entry. If there is no in label for an FTN entry, "--" is displayed.

Outgoing label: It is the out label of an ILM or FTN label. "--" indicates that an ILM or FTN label has no out label. If impl-null is shown, it indicates an implicit null label 3 and that this label is not carried in the forwarding of packets.

OP: Indicates an operation behavior that a packet hits the in label and out label of a forwarding entry (ILM or FTN). This behavior includes the following:

Field	Description
PH	Indicates that an IP packet needs to be added with labels (perhaps one to three labels) and then forwarded to the next hop after hitting the entry. Use the show mpls forwarding-table detail command to view the labels and the number of labels added. If imp-null is displayed as the out label, the imp-null label is not added in the actual forwarding process.
PP	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry, that is, perform forwarding of the last but one hop.
SW	Indicates that an MPLS packet needs to exchange labels and be forwarded to the next hop directly after hitting the entry.
SP	Indicates that an MPLS packet needs to exchange top labels, added with a label, and be forwarded to the next hop after hitting the entry. Exchanged labels are displayed for the out label field. Use the show mpls forwarding-table detail command to the labels added and the number of labels. One to two labels may be added.
PN	Indicates that an MPLS packet needs to remove the label and be forwarded to the next hop directly after hitting the entry.
PI	Indicates that an MPLS packet needs to remove all labels and be forwarded according to the destination IP address after hitting the entry.
PC	Indicates that an MPLS packet removes the top label and is forwarded according to the query result in the label forwarding table after hitting the entry. In the case of an IP packet, it is forwarded according to the destination IP address.
PM	Indicates that an MPLS packet needs to remove the label and is forwarded according to the destination MAC of the inner packet (VPLS application) after hitting the entry.
PV	Indicates that an MPLS packet needs to remove the label and is forwarded from a specified egress (VPWS application) after hitting the entry.
IP	Indicates an MPLS packet needs to be forwarded across VRFs after hitting the entry. This type of entry is the forwarding entry across VRFs of one VPN.
DP	Indicates that a packet is discarded after hitting the entry.

FEC: It has two meanings.

In the case of an FTN entry ("--" is displayed if it has no in label), the IP address and mask are displayed for the FEC field if the FTN is for IP route. If (V) is carried behind, it indicates that the FTN belongs to a VRF. In the case of a VC FTN, VC ID and VC peer IP are displayed for the FEC field.

For an ILM entry (it has an in label), if the label is for IP route, the IP address and mask are displayed for the FEC field. If (V) is carried behind, it indicates that the ILM belongs to a VRF. If the label is for a VRF of an L3 VPN (that is, each VRF of a VPN is allocated with a label), the

VRF name is displayed for the FEC field, such as VRF (vpna) in the preceding example. If the label is for VC, VC ID and VC peer IP are displayed for the FEC field, such as VC (20,1.1.1.1) in the preceding example.

Outgoing interface: Indicates the outgoing interface for packet forwarding and uses the abbreviated name of the interface.

Nexthop: Indicates the next hop for packet forwarding. "--" is displayed for a forwarding entry with an ineffective next hop address.

2) The following example shows statistics information about the process forwarding module.

```
Ruijie# show mpls forwarding-table summary
MPLS forwarding is ON
Enable count:1
ILM entrys:14
ILM changes:14
ILM failed changes :0
IP FTN entrys:0
IP FTN changes:4
IP FTN failed changes:0
L2 FTN entrys:0
L2 FTN changes:0
L2 FTN failed changes:0
In label packets:0
Out label packets:0
Send label packets:0
In ip packets:0
Out ip packets:0
Out ip stack packets:0
Forwarding packets:0
Fragment packets:0
Fragment error packets:0
Label error packets:0
Label failed packets:0
Ttl over packets:0
Buffer failed packets:0
Ip don't fragment packets:0
Other failed packets:0
```

3) The following example shows FRR information about the process forwarding module.

```
Ruijie#show mpls forwarding-table frr
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP--SWAP topmost label and push new label
DP--DROP packet
PC--POP label and continue lookup by IP or Label
PI--POP label and do ip lookup forward
```

```
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
Status codes: m - main entry, b - backup entry, * - active.
Local  Outgoing   OP  FEC            Outgoing    Nexthop
Label  label                       interface
m* --    1026      PH  120.1.1.0/24     Gi3/18      10.0.2.1
b  --    1027      PH  120.1.1.0/24     Gi3/19      10.0.3.1
m* 1028   1029      SW  120.1.2.0/24     Gi3/18      10.0.2.1
b  1028   1030      SW  120.1.2.0/24     Gi3/29      10.0.3.1
```

show mpls label-pool

Use this command to show the usage of the label pool in various label spaces. You can show the data of all the label spaces or that of a specific label space by specifying a label space number.
show mpls label-pool [*label_space*]

Parameter description

Parameter	Description
label_space	Specifies the label space whose label pool is to be shown.

Defaults N/A

Command mode Privileged mode

Usage guidelines This command shows the usage of the label pools of all label spaces or a specific label space, including the label pool size, maximum or minimum label value, and allocation of each label pool. At present, only the global label space is supported.

Examples

```
Ruijie# show mpls label-pool
label space: 0
label pool bucket size 512
min label 16, max label 1048575
label block used 2, free 2046
status codes: (s) - stale
CLI: 0   , 1    (Include label [16,1023], reserved)
LDP: 3   , 4 (s)
```

Related commands

Command	Description
label-switching	Enables label switching.

Platform description N/A

show mpls ldp bindings

Use this command to show the LDP label binding information, which can be filtered according to VRF, FEC prefix, label value, remote binding, or local binding.

show mpls ldp bindings [**all** | **vrf** *vrf-name*] [*ip-address* **|** *mask* | **label** *label*] [**remote** | **local**]

Parameter description

Parameter	Description
all	Shows label binding information under all VRFs.
vrf ***vrf-****name*	Shows label binding information under a specified VRF.
ip-address **|** *mask*	Shows label binding information of specified FECs.
label *label*	Shows label binding information of specified label values that range from 0 to 1048575.
remote	Shows remote label binding information received from the LDP peer.
local	Shows label binding information sent locally.

Defaults

No parameter is specified in this command by default, indicating that all label binding information under the global VRF is shown.

Command mode

Privileged mode

Usage guidelines

This command shows the FEC and label binding information. It shows the working status of the LDP, whether the LDP has normally bound a label to an FEC, the specific label value of bound to an FEC, and whether the binding is local binding or remote binding. If no VRF is specified, it indicates that label binding information under the global VRF is displayed.

Examples

The following example shows label database information under the global VRF.

```
Ruijie# show mpls ldp bindings
Default VRF:
  lib entry: 2.2.2.2/32
     local binding:  to lsr:10.20.10.10:0,label: imp-null
     remote binding: from lsr:10.20.10.10:0,label: 16 (not in FIB)
  lib entry: 10.20.10.10/32
     local binding:  to lsr:   10.20.10.10:0, label: 1027
     remote binding: from lsr: 10.20.10.10:0, label: imp-null
```

Field	Description
local binding	Indicates the label binding information distributed by an LSR for an FEC. "not in FIB" indicates that the information is not added to the FIB.
remote binding	Indicates the remote label binding information received from the LDP peer. "not in FIB" indicates that the information is not added to the FIB.

Related commands

Command	Description
show mpls ldp neighbor	Shows the LDP session status.

Platform description N/A

show mpls ldp discovery

Use this command to show the information about neighbors discovered by LDP under all or specified VRFs.

show mpls ldp discovery [**all** | **vrf** *vrf-name*] [**detail**]

Parameter description

Parameter	Description
all	Shows the information about neighbors discovered by LDP under all VRFs.
vrf *vrf-name*	Shows the information about neighbors by LDP under a specified VRF.
detail	Shows detailed information about neighbors discovered by LDP.

Defaults N/A

Command mode Privileged mode

Usage guidelines This command shows the interfaces on which LDP neighbors are discovered, the discovered LDP neighbors, the Hello packet source address of the LDP neighbor, and Hello keepalive time. If no VRF is specified, it indicates that the information about neighbors discovered by LDP under the global VRF is displayed.

Examples The following example shows the information about neighbors discovered by LDP under the global VRF.

```
Ruijie# show mpls ldp discovery
Default VRF:
 Local LDP Identifier:
    8.8.8.8:0
    Discovery Sources:
    Interfaces:
       GigabitEthernet 2/1 (ldp): xmit/recv
          LDP Ident: 10.30.10.10:0
       GigabitEthernet 2/2 (ldp): xmit
    Targeted Hellos:
       8.8.8.8 -> 10.5.0.1 (ldp): active, xmit
       8.8.8.8 -> 10.30.10.10 (ldp): active/passive, xmit
       2.2.2.2 -> 10.30.10.10 (ldp): passive, xmit/recv
          LDP Ident: 10.30.10.10:0
```

Field	Description

Local LDP Identifier	Indicates the LDP identifier for the local router.
Interfaces	Indicates the interface information lists discovered by the active LDP.
xmit	Indicates that Hello packets were sent on an interface.
recv	Indicates that Hello packets are received on an interface.
Targeted Hellos	Indicates the sending path list of all targeted Hello messages.
active	Indicates the local LSR actively sends targeted Hello messages.
passive	Indicates the neighbor LSR actively sends targeted Hello messages. The local LSR is configured to respond to the targeted Hello message sent by the neighbor LSR.

Related commands

Command	Description
show mpls ldp interface	Shows the LDP-enabled interface information.
neighbor *ip-address*	Creates an LDP extended peer.

Platform description N/A

show mpls ldp interface

Use this command to show information about LDP-enabled interfaces under all or specific VRFs.

show mpls ldp interface [**all** | **vrf** *vrf-name* | *interface-name*]

Parameter description

Parameter	Description
all	Shows information about LDP-enabled interfaces under all VRFs.
vrf *vrf-name*	Shows information about LDP-enabled interfaces under a specified VRF.
interface-name	Shows information about specified interfaces.

Defaults N/A

Command mode Privileged mode

Usage guidelines Use this command to show the device's interfaces on which LDP is enabled and Up/Down state of these interfaces. If no VRF is specified, it indicates that interface information under the global VRF is displayed.

Examples The following example shows information about the LDP-enabled interfaces under the global VRF.

```
Ruijie# show mpls ldp interface
Default VRF:
```

```
Interface              Operational    Status
GigabitEthernet 2/1    Yes            UP
GigabitEthernet 2/2    No             DOWN
GigabitEthernet 2/3    Yes            UP
```

Field	Description
Operational	Indicates whether an interface is enabled with LDP.
Status	Indicates the interface status.

show mpls ldp neighbor

Use this command to show information about LDP sessions under all or specified VRFs.

show mpls ldp neighbor [**all** | **vrf** *vrf-name*] [*ip-address*] [**detail**]

Parameter description

Parameter	Description
all	Shows information about LDP sessions under all VRFs.
vrf *vrf-name*	Shows information about LDP sessions under a specified VRF.
ip-address	Shows information about LDP sessions of specified LDP peers under specified or all VRFs.
detail	Shows detailed information about LDP sessions.

Defaults N/A

Command mode Privileged mode

Usage guidelines Use this command to show information about all LDP neighbors, such as the TCP connection port between the local LDP and peer LDP, LDP status, and received/sent message counts.
If no VRF is specified, information about LDP sessions under the global VRF is displayed.

Examples The following example shows the information about LDP sessions under the global VRF.

```
Ruijie# show mpls ldp neighbor
Default VRF:
 Peer LDP Ident: 10.20.10.10:0; Local LDP Ident: 8.8.8.8:0
    TCP connection: 10.20.10.10.62488 - 8.8.8.8.646
    State: OPERATIONAL; Msgs sent/recv: 42/45; UNSOLICITED
    Up time: 00:33:49
    Graceful Restart enabled; Peer reconnect time (msecs): 300000
  Down Neighbor Information:
    Status: recovering (115 seconds left)
    LDP discovery sources:
 Link Peer on GigabitEthernet 2/1,Src IP addr:192.168.201.220
```

```
Targeted Hello 8.8.8.8 -> 10.20.10.10
Addresses bound to peer LDP Ident:
  10.20.10.10   192.168.201.220 192.168.198.1   10.5.0.1
```

Field	Description
Peer LDP Ident	Indicates the peer LDP identifier of an LDP session.
Local LDP Identifier	Indicates the LDP identifier of the local router.
TCP connection	Indicates the TCP connection that supports the LDP session.
State	Indicates the LDP session state.
Msgs sent/recv	Count of LDP messages which are sent to and received from the session peer
UNSOLICITED&ONDEMAND	Indicates the label distribution mode.
Up time	Indicates the time when an LDP session is established.
Graceful Restart enabled	Indicates that Graceful Restart is enabled.
Peer reconnect time (msecs)	Indicates the reconnect time of the peer LDP session.
Down Neighbor Information	Indicates the neighbor down information.
Status	Indicates that the neighbor is recovering and 115 seconds are left before the neighbor is recovered.

Related commands

Command	Description
show mpls ldp discovery	Shows the information about neighbors discovered by LDP.

Platform description N/A

show mpls ldp parameters

Use this command to show LDP configuration parameters under all or specified VRFs.

show mpls ldp parameter [**all** | **vrf** *vrf-name*]

Parameter description

Parameter	Description
all	Shows LDP configuration parameters under all VRFs.
vrf *vrf-name*	Shows LDP configuration parameters under a specified VRF.

Defaults N/A

Command mode Privileged mode

Usage guidelines Use this command to show various attributes of LDP, including the LSR ID, transport address, loop detection mechanism, label distribution and control mode, label retention mode, interval and

holdtime of the Hello packet for the extended mechanism, and interval and holdtime of the keepalive packet. If no VRF is specified, it indicates that configuration parameters of LDP under the global VRF are displayed.

Examples The following example shows configuration parameters of LDP under the global VRF:

```
Ruijie# show mpls ldp parameters
Default VRF:
  Protocol version: 1
    Ldp Router ID: 1.1.1.1
    Control Mode: INDEPENDENT
    Propogate Release: FALSE
    Label Merge: TRUE
    Label Retention Mode: LIBERAL
    Loop Detection Mode: off
    Targeted Session Keepalive HoldTime/Interval: 180/60 sec
    Targeted Hello HoldTime/Interval: 45/5 sec
    LDP initial/maximum backoff: 15/120 sec
```

Related commands

Command	Description
ldp router-id	Configures the LDP router ID.
ldp-control-mode	Configures the LDP control mode.
ldp-label-retention -mode	Configures the label retention mode.
propagate-release	Configures the label propagate release switch.
label-merge	Configures the label merge switch.
loop-detection-mode	Configures loop detection.

Platform description N/A

show mpls rib

Use this command to show the MPLS RIB information.

show mpls rib [**all** | **vrf** *vrf-name*]

Parameter description

Parameter	Description
all	Shows MPLS routing information under all VRFs.
vrf *vrf-name*	Shows MPLS routing information under a specified VRF.

Defaults N/A

Command mode Privileged mode

Usage guidelines If no parameter is specified in this command, it indicates that MPLS routing information under the global VRF is displayed.

Examples The following example shows the MPLS routing information under the global VRF.

```
Ruijie#show mpls rib
Status codes: m – main entry, b – backup entry, * – active, s – stale.
Default VRF:
LSP Information    Total
STATIC LSP         0
LDP LSP            3
RSVP LSP           0
BGP LSP            0
L3VPN LSP          0
LDP LSP:
------------------------------------------------------------------------
FEC            In/Out Label     In/Out IF       Nexthop
119.1.1.0/24    -/1025           -/Gi3/19        10.0.10.1
m* 120.1.1.0/24    -/1026           -/Gi3/18        10.0.2.1
b  120.1.1.0/24    -/1031           -/Gi3/19        10.0.10.1
m* 120.1.2.0/24    1027/1032        Gi3/10/Gi3/18   10.0.2.1
b  120.1.2.0/24    1027/1033        Gi3/10/Gi3/19   10.0.10.1
------------------------------------------------------------------------
```

Field	Description
LSP Information	Shows the LSP information. STATIC LSP: This type of LSP is configured manually. LDP LSP: This type of LSP is established by using LDP. RSVP LSP: This type of LSP is an MPLS TE tunnel established by using RSVP-TE. BGP LSP: This type of LSP is established by using BGP for IPv4 private network BGP routes or IPv4 public network BGP routes. L3VPN LSP: This type of LSP is established by using BGP for received VPNv4 routes.
Total	Shows the total amount of LSP information related to a VRF.
FEC	Shows the FEC, whose value is usually the destination address of an LSP.
In/Out Label	Shows the value of the in/out label
In/Out IF	Shows the name of the in/outgoing interface
Nexthop	Shows the next hop

Related commands

Command	Description
N/A	N/A

Platform description N/A

show mpls summary

Use this command to show the MPLS global configuration information.

show mpls summary

Parameter description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged mode

Usage guidelines This command shows the basic information about MPLS, including the maximum/minimum available labels, information about each label space, label space used by each interface, and total number of MPLS-enabled interfaces.

Examples

```
Ruijie# show mpls summary
Per label-space information://Information about each label space.
Currently, only label space 0 is supported.
Label-space 0 is using minimum label:16 and maximum label:1048575//Label
scope allowed by this label space
Label-switching Interface://Interface enabled with label switching
Interface              Label space
GigabitEthernet 4/1      0
GigabitEthernet 4/2      0
Total number of mpls interface is 2
```

Related commands

Command	Description
label-switching	Enables label switching.

Platform description N/A

show mpls tunnel-info

Use this command to show tunnels over a public network. Use the **no** form of this command to remove the configuration.

show mpls tunnel-info { **all** | *tunnel-id* }

Parameter

Parameter	Description

description	**all**	Shows all tunnels over a public network.
	tunnel-id	Specifies a tunnel.

Defaults N/A

Command mode Priviledged EXEC mode

Usage guidelines All tunnels over the public network are up. Therefore, the tunnel status is not shown.

Examples The following example shows tunnels over a public network.

```
Ruijie# show mpls tunnel-info all
Total tunnel-info num:3
LSP tunnel-info num:2
GRE tunnel-info num:1
RSVP-TE tunnel-info num:0
Tunnel-ID     Type       Destination
0x00000001    LSP        4.4.4.4/32
0x00000002    LSP        3.3.3.3/32
0x00000004    GRE        2.2.2.2/32

Ruijie# show mpls tunnel-info 1
Tunnel-ID: 0x00000001
Type: LSP
Destination: 4.4.4.4/32
Reserved for bind: false
FTN-IX: 0x00000001
Owner: LDP

Ruijie# show mpls tunnel-info 4
Tunnel-ID: 0x00000004
Type: GRE
Destination: 2.2.2.2/32
Reserved for bind: false
Interface name: Tunnel 1
```

Related commands	**Command**	**Description**
	N/A	N/A

Platform description N/A

show mpls tunnel-policy

Use this command to show the tunnel policy. Use the **no** form of this command to remove the configuration.

show mpls tunnel-policy { **all** | **name** *policy-name* }

Parameter description

Parameter	Description
all	Shows all tunnel policies.
name *policy-name*	Specifies a tunnel policy.

Defaults N/A

Command mode Priviledge EXEC mode

Usage guidelines N/A

Examples The following example shows all tunnel policies.

```
Ruijie# show mpls tunnel-policy all
Total tunnel policy num: 4
Select tunnel policy num: 1
Binding tunnel policy num: 1
Invalid tunnel policy num: 2

Tunnel policy name         Select-Seq
pol_sel                    LSP

Tunnel policy name         Binding type  Tunnel-interface
pol_bind                  GRE          tunnel 1

Invalid tunnel policy:
  pol-name1, pol-name2
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

snmp-server enable traps mpls

Use this command to enable trap transmission of MPLS. Use the **no** form of this command to disable trap transmission of MPLS.

snmp-server enable traps mpls {xc|ldp|vpn}

snmp-server enable traps mpls xc [xc-up] [xc-down]

snmp-server enable traps mpls ldp [pv-limit][session-down][session-up]

snmp-server enable traps mpls l3vpn [max-threshold] [mid-threshold][max-thresh-cleared][vrf-up][vrf-down]

no snmp-server enable traps mpls xc [xc-up] [xc-down]

no snmp-server enable traps mpls ldp [pv-limit][session-down][session-up]

no snmp-server enable traps mpls l3vpn [max-threshold] [mid-threshold][max-thresh-cleared][vrf-up][vrf-down]

Parameter description

Parameter	Description
xc	Indicates the trap transmission switch for MPLS route change.
ldp	Indicates the trap transmission switch for LDP.
l3vpn	Indicates the trap transmission switch for L3 VPN.
xc-up	Indicates the trap transmission switch for MPLS route change XC Up.
xc-down	Indicates the trap transmission switch for MPLS route change XC Down.
pv-limit	Indicates the trap transmission switch for mismatch of path vectors.
session-down	Indicates the trap transmission switch for disconnected LDP sessions.
session-up	Indicates the trap transmission switch for created LDP sessions
max-threshold	Indicates the Trap transmission switch for VRF maximum route threshold.
mid-threshold	Indicates the Trap transmission switch for VRF middle route threshold.
max-thresh-cleared	Indicates the Trap transmission switch for cleared VRF maximum route threshold.
vrf-up	Indicates the trap transmission switch for VRF Up.
vrf-down	Indicates the trap transmission switch for VRF Down.

Defaults

Traps of MPLS are not transmitted by default.

Command mode

Global configuration mode

Usage guidelines

There are two types of XC traps:

- XC Up trap, indicating that an effective ILM or FTN entry is generated

- XC Down trap, indicating that an ILM or FTN entry is deleted

You can enable the preceding two trap switches at the same time by using the **snmp-server enables mpls xc** command, or either of these switches by using the **snmp server enables mpls xc [xc-up] [xc-down]** command.

There are three types of LDP traps:

- LDP session Up trap, which is sent when an LDP session is established
- LDP session Down trap, which is sent when an LDP session is disconnected
- When initialization messages (INIT) are exchanged after an LDP session is established, a trap is sent if the value of the path vector list length used in loop detection does not match that advertised by the neighbor.

You can enable the preceding three trap switches at the same time by using the **snmp-server enables mpls ldp** command or any of these switches by using the **snmp server enables mpls ldp [pv-limit] [sesseion-up] [session-down]** command.

There are the following types of L3 VPN traps:

- Trap identifying VRF Up or Down: When an VRF instance has an associated interface up, the VRF instance is considered to be in Up state. In this case, a VRF Up trap is sent. When an VRF instance has all its associated interfaces down or has no associated interface, a VRF Down trap is sent.
- Trap of VRF route pre-alert: When the number of VRF routes exceeds the middle route capacity, a VRF MidThreshExceed trap is sent. When the number of VRF routes exceeds the maximum route capacity, a VRF MaxThreshExceed trap is sent. In this case, a VRF MaxThreshCleared trap is sent after the number of VRF routes is below the maximum route capacity, indicating that the number of VRF routes returns to normal.

You can enable all trap switches for L3 VPN at the same time by using the **snmp-server enables mpls l3vpn** command or any of these switches by using the **snmp server enables mpls l3vpn [max-threshhold] [mid-threshhold][max-thresh-cleared] [vrf-up] [vrf-down]** command.

To capture a trap on a host after MPLS trap transmission is enabled, you must use the **snmp-server host c**ommand to specify the host that receives the trap.

Examples

The following example enables trap transmission of LDP.

```
Ruijie(config)#snmp-server host 192.168.10.1
Ruijie(config)#snmp-server enable traps mpls ldp
```

Related commands

Command	Description
snmp-server host	Sets a host for receiving traps.

Platform description

N/A

target-session holdtime

Use this command to set the keepalive holdtime for the extended mechanism. Use the **no** form of this command to restore the default value.

target-session holdtime *seconds*

Parameter description

Parameter	Description
seconds	Sets the holdtime in seconds. The range is from *15 to 65535.*

Defaults The holdtime of the LDP session established by the extended discovery mechanism is 180 seconds by default. The sending interval of the keepalive message is 60 seconds by default, which is 1/3 of the session holdtime.

Command mode config-mpls-router mode

Usage guidelines This command is valid for only the LDP sessions established by the extended discovery mechanism after configuration of this command.

Examples The following example configures the keepalive holdtime for LDP sessions established by the extended mechanism.

```
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)# target-session holdtime 90
```

Related commands

Command	Description
show mpls ldp parameters	Shows LDP configuration parameters under all or specified VRFs.

Platform description N/A

Platform description N/A

traceroute mpls

Use this command to detect an MPLS LSP hop by hop and trace the LSRs on the LSP.
traceroute mpls ipv4 *ip-address*/*mask* [**timeout** *timeout*] [**ttl** *time-to-live*] [**source** *ip-address*] [**destination** *ip-address*] [**force-explicit-null**] [**reply mode** {**ipv4 | router-alert**}] [**flags fec**] [**verbose**]

Parameter description

Parameter	Description
ip-address/mask	Specifies the IPv4 address and subnet mask length of the destination FEC to be tested
timeout timeout	(Optional) Specifies the timeout time for a packet. The range is from 0 to 3600. The default value is 2.

ttl time-to-live	(Optional) Specifies the TTL value for sending packets. The range is from 1 to 255. The default value is 30.
source ip-address	(Optional) Specifies the source address. It is the destination address when the peer sends an Echo Reply packet.
destination ip-address	(Optional) Specifies the 127/8 segment address. It is used to pad the IP header, 127.0.0.1 by default.
force-explicit-null	(Optional) Indicates whether an explicit null label is forcibly added to the MPLS label. An explicit null label is not forcibly added to the MPLS label by default.
reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode of the Echo Request packet: **ipv4**: Reply with an IPv4 UDP packet. It is the default value. **router-alert**: Reply with an IPv4 UDP packet with the Router Alert option.
flags fec	(Optional) Enables the forcible FEC stack check.
verbose	(Optional) Shows detailed information about Echo Reply packets. The information is not shown by default.

Defaults See the preceding parameter description.

Command mode Privileged mode

Usage guidelines You can change some default parameter values by specifying optional parameters. You can either directly type this command or enter the interactive typing mode by pressing Enter after typing the **traceroute mpls** command.

Examples The following example shows the LSRs on the LSP of the FEC corresponding to 10.10.10.10/32.

```
Ruijie# traceroute mpls ipv4 10.10.10.10/32
Tracing MPLS Label Switched Path to 10.10.10.10/32, timeout is 2 seconds
       < press Ctrl+C to break >
Codes:'!' - success,'Q' - request not sent,'.'-timeout,
  'L'-labeled output interface,'B'-unlabeled output interface,
  'D'-DS Map mismatch,'F'-no FEC mapping,'f'-FEC mismatch,
  'M'-malformed request,'m'-unsupported tlvs,'N'-no label entry,
  'P'-no rx intf label prot,'p'-premature termination of LSP,
  'R'-transit router,'I'-unknown upstream index,
  'X'-unknown return code,'x'-return code 0
Type escape sequence to abort.
  0 10.3.0.8 MRU 1500 [Labels: 17 Exp: 0]
L 1 10.3.0.1 MRU 1504 [Labels: implicit-null Exp: 0] 624 ms
! 2 10.2.0.1 708 ms
```

See the **ping mpls** command for descriptions of return values.

Related commands	Command	Description
	ping mpls	Detects the connectivity of an MPLS LSP.

Platform description N/A

transport-address

Use this command to configure globally the transport address used by basic LDP sessions. Use the **no** form of this command to delete the configuration.

transport-address {interface | *ip-address* **|** *interface-name* **}**

no transport-address

Parameter description	Parameter	Description
	interface	Indicates that the primary IP address of an interface is used as the transport address for basic LDP sessions established on each interface.
	Ip-address	Indicates that the specified IP address is used as the transport address for all basic LDP sessions.
	Interface-name	Indicates that the primary IP address of the specified interface is used as the transport address for all basic LDP sessions.

Defaults The LSR ID of LDP is used as the transport address by default.

Command mode config-mpls-router mode

Usage guidelines This command is valid for only LDP sessions established by the extended discovery mechanism instead of the basic discovery mechanism. LDP sessions established by the extended discovery mechanism always use the LSR ID of LDP as the transport address. If both an interface transport address and a global transport address are configured, the interface transport address takes precedence over the global transport address.

Examples The following example configures the primary IP address of each interface as the transport address.

```
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)# transport-address interface
```

Related commands	Command	Description
	mpls ldp transport-address	Configures the transport address used by basic LDP sessions established on an interface.

Platform N/A

description

tunnel-policy

Use this command to create a tunnel policy. Use the **no** form of this command to remove the configuration.

tunnel-policy *policy-name*

no tunnel-policy *policy-name*

Parameter description

Parameter	Description
policy-name	Configures the policy name, in the range from 1-31 characters (case-sensitive)

Defaults N/A

Command mode Global configuration mode

Usage guidelines N/A

Examples The following example configures tunnel named tnl-pol.

```
Ruijie(config)# tunnel-policy tnl-pol
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

tunnel binding

Use this command to configure a tunnel binding policy. Use the **no** form of this command to remove the configuration.

tunnel binding gre *interface-name*

no tunnel binding gre *interface-name*

Parameter description

Parameter	Description
gre	Binds a GRE tunnel.
interface-name	Configures an interface name.

Defaults N/A

Command mode Tunnel policy mode

Usage guidelines

The binding policy and selection policy cannot be both configured.

The bound tunnel must be global. The tunnel interface cannot be bound to a VRF.

The tunnel type must be consistent with the encapsulation type. Otherwise, the policy does not take effect.

Examples The following example configures a tunnel binding policy for GRE tunnel 1.

```
Ruijie(config)# tunnel-policy tnl-pol
Ruijie(config-tunnel-policy)# tunnel binding gre tunnel 1
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

tunnel select

Use this command to configure a tunnel selection policy. Use the **no** form of this command to remove the configuration.

tunnel select lsp

no tunnel select

Parameter description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Tunnel policy mode

Usage guidelines The binding policy and selection policy cannot be both configured.

Examples The following example configures a tunnel selection policy.

```
Ruijie(config)# tunnel-policy tnl-pol
Ruijie(config-tunnel-policy)# tunnel select lsp
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

BGP/MPLS L3 VPN Commands

address-family(VRF)

Use this command to configure the IPv4 or IPv6 address family for the multi-protocol VRF.

address-family {ipv4 | ipv6}

Parameter Description

Parameter	Description
N/A	N/A

Defaults No IPv4 or IPv6 address family is configured for the multi-protocol VRF by default.

Command Mode VRF configuration mode

Usage Guide Configuring the IPv4 address family for the multi-protocol VRF is equivalent to enabling the IPv4 protocol. Configuring the IPv6 address family for the multi-protocol VRF is equivalent to enabling the IPv6 protocol.

Configuration Examples The following example defines the multi-protocol VRF vrf1 and configures the 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 configuration mode for the VRF address family.
vrf definition	Defines the multi-protocol VRF.

Platform Description N/A

address-family ipv4 vrf (BGP)

Use this command to enter VRF address family mode to enable routing information exchange for a VRF.

Use the **no** form of this command to exit VRF address family mode.

address-family ipv4 vrf *vrf-name*

no address-family ipv4 vrf *vrf_name*

Parameter Description

Parameter	Description
vrf-name	Name of the VRF

Defaults No VRF address family is defined by default.

Command Mode BGP configuration mode

Usage Guide Use this command to enable (or disable) routing information exchange between the PE and CE.
Use the **exit-address-family** command to return to BGP configuration mode.

Configuration Examples

```
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family ipv4 vrf vrf1
```

Related Commands

Command	Description
neighbor activate	Activates an address family.
exit-address-family	Exits this mode.

Platform Description N/A

address-family ipv6 vrf (BGP)

Use this command to enter VRFv6 address family mode to enable IPv6 routing information exchange for a VRF.
Use the **no** form of this command to exit VRFv6 address family mode.
address-family ipv6 vrf *vrf-name*
no address-family ipv6 vrf *vrf_name*

Parameter Description

Parameter	Description
vrf-name	Name of the VRF

Defaults No VRFv6 address family is defined by default.

Command Mode BGP configuration mode

Usage Guide Use this command to enable (or disable) routing information exchange between the PE and CE.
Use the **exit-address-family** command to return to BGP configuration mode.

Configuration Examples

```
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family ipv6 vrf vrf1
```

Related Commands

Command	Description
neighbor activate	Activates an address family.
exit-address-family	Exits this mode.

Platform Description N/A

address-family vpnv4 (BGP)

Use this command to enter VPN address family mode to enable VPN routing information exchange between PEs.

Use the **no** form of this command to exit VPN address family mode.

address-family vpnv4 [**unicast**]

no address-family vpnv4 [**unicast**]

Parameter Description

Parameter	Description
unicast	Specifies the unicast address prefix.

Defaults No vpn address family is defined by default.

Command Mode Router mode

Usage Guide Use this command to enable VPN routing information exchange between PEs and enter **address-family VPN** mode. Use the **exit-address-family** command to exit **address-family VPN** configuration mode.

Configuration Examples

```
Ruijie(config)# router bgp 100
Ruijie (config-router)# address-family vpnv4
```

Related Commands

Command	Description
neighbor activate	Activates an address family.
exit-address-family	Exits this mode.

Platform Description N/A

address-family vpnv6 (BGP)

Use this command to enter VPNv6 address family mode to enable VPNv6 routing information exchange between PEs.

Use the **no** form of this command to exit VPNv6 address family mode.

address-family vpnv6 [**unicast**]

no address-family vpnv6 [**unicast**]

Parameter Description

Parameter	Description
unicast	Specifies the unicast address prefix.

Defaults No VPNv6 address family is defined by default.

Command Mode BGP configuration mode

BGP scope mode

Usage Guide Use this command to enable VPNv6 routing information exchange between PEs and enter **address-family VPNv6** mode. Use the **exit-address-family** command to exit **address-family VPN v6** configuration mode.

Configuration Examples

```
Ruijie(config)# router bgp 100
Ruijie (config-router)# address-family vpnv6
```

Related Commands

Command	Description
neighbor activate	Activates an address family.
exit-address-family	Exits this mode.

Platform Description N/A

alloc-label

Use this command to configure the label allocation method for VPNs.

alloc-label {**per-vrf** | **per-route**}

no alloc-label {**per-vrf** | **per-route**}

Parameter Description

Parameter	Description
per-vrf	Allocates a label for each VPN.
per-route	Allocates a label for each VPN route.

Defaults A label is allocated for each VRF by default.

Command Mode VRF configuration mode

Usage Guide RFC4364 outlines two label allocation methods for L3VPN: a label for each route and a label for each VRF. The former method rapidly forwards packets to the next hop by searching the ILM table based on the label, but it requires a large ILM table. For the latter method, all routes of a VRF share the label, which significantly reduces the size of the ILM table, but its forwarding efficiency is lower for it performs table search twice. First it searches the ILM table for the VRF of a packet, then searches the routing table of the VRF for the destination IP address to which it forwards the packet.

Configuration Examples The following example configures label allocation per route for VPNA.

```
Ruijie(config)# ip vrf VPNA
Ruijie(config-vrf)# alloc-label per-route
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

area sham-link

Use this command to configure a sham link.
Use the **no** form of this command to delete the specified sham link.
area *area-id* **sham-link** *source-address destination-address* [**cost** *number*] [**dead-interval** *seconds*] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**authentication** [**message-digest | null**]] [[**authentication-key** [**0**|**7**] *key*] **|** [**message-digest-key** *key-id* **md5** [**0**|**7**] *key*]]
no area *area-id* **sham-link** *source-address destination-address* [**cost**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**authentication**] **[**[**authentication-key**] **|** [**message-digest-key** *key-id*]]

Parameter Description

Parameter	Description
area-id	OSPF area ID of the sham link. It can be a decimal integer ranging from 0 to 4294967295 or an IP address.
source-address	Sham link source address
destination-address	Sham link destination address

cost *number*	(Optional) COST value for OSPF to send packets on the sham link. It ranges from 0 to 65535 with the default value of 1.
dead-interval *seconds*	(Optional) Interval at which the neighbor of the sham link dies. It ranges from 0 to 2147483647 with the default value of 40 seconds.
hello-interval *seconds*	(Optional) Interval of sending the Hello packet on the sham link. It ranges from 1 to 65535 with the default value of 10 seconds.
retransmit-interval *seconds*	(Optional) Interval of retransmitting packets on the sham link. It ranges from 0 to 65535 with the default value of 5 seconds.
transmit-delay *seconds*	(Optional) Delay for transmitting the LSU packet on the sham link. It ranges from 0 to 65535, with the default value of 1 second.
authentication-key *key*	(Optional) Defines the key for OSPF plain text authentication. The keys for plain text authentication between neighbors must be consistent. Use the **service password-encryption** command to display the key in encrypted mode. 0: The key is displayed in plain text. 7: The key is displayed in encrypted text.
message-digest-key *key-id* **md5** key	(Optional) Defines the key identifier and key for OSPF MD5 authentication. The key identifiers and keys for MD5 authentication between neighbors must be consistent. Use the **service password-encryption** command to display the key in encrypted mode. 0: The key is displayed in plain text. 7: The key is displayed in encrypted text.
authentication	Sets the authentication type to plain text authentication.
message-digest	Sets the authentication type to MD5 authentication.
null	Sets authentication not to be carried out.

Defaults Authentication is not carried out by default.

Command Mode OSPF Router mode

Usage Guide This command is valid only for OSPF instances associated with the VRF.

To configure a sham link, configure the two PEs between which the sham link is to be established. If you configure only one PE, the sham link cannot be established.

To establish a sham link between the two PEs, the following configuration requirements must be met:

- The sham link area-id on the two PEs must be the same.
- The source address of the sham link configured on one PE must be the destination address of the sham link configured on the other PE.
- The source address of the sham link configured on the PE must be a 32-bit loopback address, and this address must be bound to the corresponding VRF instance.

As the OSPF route announced through the sham link does not contain a VPN tag, this route cannot be used for forwarding. The actual forwarding still needs to use the BGP VPNv4 route. Therefore, during the actual configuration, ensure that the route announced through the sham link can announce

the VPNv4 route to the related BGP neighbor through the MP-BGP protocol.


Caution

The source address for establishing a sham link must participate in the BGP VPNv4 route announcement, but cannot participate in the calculation of the VRF OSPF instance.

Configuration Examples The following example configures a sham link for an OSPF instance. The sham link belongs to the area 0, the source address is 1.1.1.1, the destination address is 2.2.2.2, and the COST value for transmitting packets on the sham link by the OSPF protocol is 10.

```
Ruijie(config)# router ospf 10 vrf vpn1
Ruijie(config-router)# area 0 sham-link 1.1.1.1 2.2.2.2 cost 10
```

Related Commands

Command	Description
show ip ospf sham-links	Displays all sham link information of the OSPF instance.

Platform Description N/A

bgp default route-target filter

Use this command to enable automatic router-target filtering of BGP.
Use the **no** form of this command to disable the function.

bgp default route-target filter

no bgp default route-target filter

Parameter Description

Parameter	Description
N/A	N/A

Defaults Automatic router-target filtering of BGP is enabled by default.

Command Mode BGP configuration mode

Usage Guide By default, a PE denies a VPN route from another PE or ASBR if the VPN route is not imported by any of its VRFs. Use the **no** form of this command to allow a PE to accept all VPN routes from other PEs or ASBRs, regardless of whether its VRFs import the VPN routes.
This command is used for inter-domain VPN OptionB solution. Because no VRF is configured on an ASBR, but the ASBR needs to save VPN routes and announce them to other PEs (or ASBRs), you

need to run the **no bgp default route-target filter** command.


Caution

After the BGP peers are established and VPN routes are distributed, changing this configuration takes effect only for VPN routes received after the change but not for VPN routes that have already been accepted or denied. It is recommended to use the **clear ip bgp** command to reset the sessions with the BGP peers, exchange VPN routes again, and determine whether to accept VPN routes.

For example, you have run the **bgp default route-target filter** command to enable automatic route-target filtering. After the BGP peers are established and VPN routes are distributed, you want to disable this function. In this case, run the **no bgp default route-target filter** command, then run the **clear ip bgp** command to reset the sessions with the BGP peers.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

capability vrf-lite

Use this command to control the loop inspection of the OSPF instance.

Use the **no** form of this command to enable loop inspection.

Use the **default** form of this command to restore to the default configuration.

capability vrf-lite [**auto**]

no capability vrf-lite [**auto**]

[**default**] **capability vrf-lite** [**auto**]

Parameter Description

Parameter	Description
auto	The OSPF instance associated with the VRF automatically determines whether to support loop inspection.

Defaults The OSPF instance associated with the VRF automatically determines whether to support loop inspection by default.

Command Mode OSPF Router mode

Usage Guide This command is valid only for the OSPF instance associated with the VRF.

By default, the OSPF instance associated with the VRF automatically determines whether to support loop inspection and the PE-CE OSPF feature. Run the **capability vrf-lite** command to forcibly

disable the preceding functions. Run the **no capability vrf-lite** command to forcibly enable the preceding functions. Run the **capability vrf-lite auto** command to allow the OSPF instance associated with the VRF to automatically determine whether to enable the preceding functions. Run the **default capability vrf-lite auto** command to restore to the default configuration.

Loop inspection of the OSPF instance is to prevent the possible loop during transmission through the VPN route. The OSPF instance associated with the VRF processes the received LSAs according to the rules in the following table.

LSA Type	Processing
Types 3, 5, and 7	Inspects the DN bit. If the received LSA has a DN bit, the LSA will not participate in the OSPF calculation.
Types 5 and 7	Inspects the VPN domain-tag. If the VPN domain-tag of the received LSA and the VPN domain-tag of the local OSPF instance are the same, the LSA will not participate in the OSPF calculation.

If loop inspection is disabled, the OSPF protocol will not inspect the DN bit and the VPN domain-tag in a received LSA packet, and it will let the LSA participate in the OSPF calculation.

The PE-CE OSPF feature is used to convert different OSPF LSAs to CE based on the BGP extension attribute. (For details about the PE-CE OSPF feature, see the *MPLS Configuration Guide*.) If the PE-CE OSPF feature is disabled, different OSPF LSAs are not converted based on the BGP attribute.

By default, the OSPF instance associated with the VRF automatically determines whether to support loop inspection.

Loop inspection of the VRF OSPF instance may need to be disabled in certain scenarios. For example, a VPN user uses an MCE device to exchange VPN routes with a PE. If the OSPF protocol runs for VPN route exchange between the MCE and PE, loop inspection of the VRF OSPF instance on the MCE device must be disabled to allow the MCE to learn VPN routes issued by the PE and send the learned VPN routes to downstream VPN sites. In a normal MCE scenario, a Ruijie device can automatically determine the situation and disable loop detection of the OSPF instance. If the device determines the situation incorrectly, you need to run the [**no**] **capability vrf-lite** command to forcibly enable or disable loop detection of the OSPF instance.

Configuration Examples

The following example disables loop inspection of the OSPF instance.

```
Ruijie(config)# router ospf 10 vrf vpn1
Ruijie(config-router)# capability vrf-lite
```

Related Commands

Command	Description
domain-tag	Configures domain-tag information of the OSPF instance.

Platform Description

N/A

clear ip bgp vrf

Use this command to reset the sessions of all members in the VRF.

clear ip bgp vrf *vrf-name* {* | *address* | *as-num*} [[**soft**] [**in** | **out**]]

Parameter Description

Parameter	Description
vrf-name	Name of the VRF
*	Resets all BGP sessions in the VRF.
address	Resets the BGP sessions with the specified peer in the VRF.
as-num	as number that identifies the peer
in	Resets the actively-connected session bulit by the peer.
out	Resets the actively-connected session bulit by the local BGP speaker.
soft	Soft resets the route information sent to or received from the specified peer.
soft in	Soft resets the received route information.
soft out	Soft resets the distributed route information.

Defaults N/A.

Command Mode Privileged EXEC mode

Usage Guide Use this command to reset the BGP sessions of all members in the VRF.

Configuration Examples

```
Ruijie# clear ip bgp vrf my-vrf in
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

description

Use this command to set the VRF descriptor.

description *string*

Parameter Description

Parameter	Description
string	A string containing a maximum of 244 characters

Defaults N/A

Command Mode VRF configuration mode

Usage Guide N/A

Configuration Examples The following example defines a single-protocol IPv4 VRF vrf1 and sets the descriptor to vpn-a.

```
Ruijie(config)#ip vrf definition vrf1
Ruijie(config-vrf)#description vpn-a
```

The following example defines a multi-protocol VRF vrf2 and sets the descriptor 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 multi-protocol VRF.

Platform Description N/A

disable-dn-bit-check

Use this command to disables check for DN bit of OSPF LSA. Use the **no** form of this command to remove the configuration.

disable-dn-bit-check [**ase | nssa | summary**]

no disable-dn-bit-check [**ase | nssa | summary**]

Parameter description

Parameter	Description
ase	Disables check for DN bit of AS-external-LSA
nssa	Disables check for DN bit of NSSA LSA
summary	Disables check for DN bit of Summary LSA

Defaults Check for the DN bit is enabled by default.

Command mode OSPF router mode

Usage guidelines This command is valid for the OSPF instance associated with VRF.
This command may cause routing loops. It is recommended to run this command in specific scenarios.

Examples The following example disables check for DN bit of AS-external-LSA in a VRF OSPF instance.

```
Ruijie(config)# router ospf 10 vrf vpn1
Ruijie(config-router)# disable-dn-bit-check ase
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

domain-id

Use this command to configure the domain ID of the OSPF instance.
Use the **no** form of this command to delete the domain ID of the OSPF instance.
domain-id {*ip-address* [**secondary**] **| null | type** {**0005|0105|0205|8005**} **value** *hex-value* [**secondary**]}
no domain-id [*ip-address* [**secondary**] **| null | type** {**0005|0105|0205|8005**} **value** *hex-value* [**secondary**]]

Parameter Description

Parameter	Description
ip-address	Sets the domain ID to an IP address.
secondary	The configured domain ID serves as the secondary identifier.
null	The OSPF instance has no domain ID.
type {0005|0105|0205|8005}	Sets the domain ID type of the OSPF instance. The following four values are available: 0x0005, 0x0105, 0x0205, and 0x8005. The default type is 0x0005.
value *hex-value*	Sets the domain ID of the OSPF instance, which is a hexadecimal numeral containing six bytes.
secondary	The configured domain ID serves as the secondary identifier.

Defaults The domain-id value of the OSPF instance is NULL and the type is 0005 by default.

Command Mode OSPF Router mode

Usage Guide This command is valid only for the OSPF instance associated with the VRF.
Assume that the OSPF instance is configured with a domain ID. When an OSPF route changes to a VPN route after being redistributed to the BGP, the domain ID is also redistributed to the BGP, and is finally announced to other PEs as a part of the extended community attribute of the VPN route.
An OSPF instance can be configured with multiple domain IDs by using the **domain-id secondary** command. However, there is only one primary domain ID, and others are secondary domain IDs. When the OSPF route is converted to the VPN route and announced, the related extended community attribute carries only the primary domain ID information.
Generally, the OSPF protocol runs between the PE and CE to exchange VPN routes. After receiving the VPN route and redistributing it to the OSPF instance, the PE announces this to VPN sites as type 5 LSA. However, for different sites that belong to the same OSPF domain, the route should be announced as type 3 LSA. You can configure the same domain ID for the related VRF OSPF instance on the PE to enable the route inside the domain to be announced as type 3 LSA.
On one PE, domain IDs of different VRF OSPF instances do not affect each other. They can be the same or different. However, the VRF OSPF instances that belong to one VPN must be configured with the same domain ID to ensure correct route announcement.

Configuration Examples The following example configures the domain ID of the VRF OSPF instance.

```
Ruijie(config)# router ospf 10 vrf vpn1
Ruijie(config-router)# domain-id type 0005 value 000000000001
```

Related Commands

Command	Description
show ip ospf	Displays the summary information of the OSPF instance.

Platform Description N/A

domain-tag

Use this command to configure the VPN domain-tag of the OSPF instance associated with the VRF.
Use the **no** form of this command to restore the default value of the VPN domain-tag of the OSPF instance.

domain-tag *tag*

no domain-tag

Parameter Description

Parameter	Description
tag	The domain-tag value of the OSPF instance, in the range from 1 to 4294967295

Defaults The default value of the VRF OSPF instance is the AS number of the local BGP protocol.

Command Mode OSPF Router mode

Usage Guide This command is valid only for the OSPF instance associated with the VRF and the BGP redistributed route.

If a VPN site connects to multiple PEs, the VPN site learns the VPN route from PEs through MP-BGP. If the VPN route is announced to the VPN site as type 5 or type 7 LSA, which may be learned by other PE routers connected to the VPN site and announced, a loop may occur. To prevent such a loop, configure the same VPN domain-tag for the VRF OSPF instances connected to the same VPN site on PEs. When the VRF OSPF instance sends type 5 or type 7 LSA to VPN sites, the LSA is attached with the VPN domain-tag information. When another PE site receives this type 5 or type 7 LSA and detects that the VPN domain-tag in the LSA is identical to the VPN domain-tag of the local OSPF instance, it does not let the LSA participate in OSPF calculation.

Generally, the OSPF instances that belong to the same VPN are configured with the same tag value. A VPN domain-tag contains four bytes in an OSPF packet. If this command is not configured for a VRF OSPF instance, by default, when the OSPF instance announces type 5 or type 7 LSA, the former two bytes of the VPN domain-tag are set to 0xD000, and the latter two bytes are set to the AS number of the local BGP. For example, if the AS number of the local BGP is 1, the hexadecimal value of the VPN domain-tag is 0xD0000001.

Configuration Examples The following example sets the domain-tag value of the OSPF instance to 10.

```
Ruijie(config)# router ospf 10 vrf vpn1
Ruijie(config-router)# domain-tag 10
```

Related Commands

Command	Description
capability vrf-lite	Controls loop inspection.

Platform Description N/A

exit-address-family (BGP)

Use this command to exit VRF family address configuration or vpn family address configuration mode.

exit-address-family

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Specific address family configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family vpnv4 unicast
Ruijie(config-router-af)# exit-address-family
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

exit-address-family(VRF)

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 creates a multi-protocol 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

Command	Description

Commands		
	address-family	Configures an IPv4 or IPv6 address family for a multi-protocol VRF.
	vrf definition	Defines a multi-protocol VRF.

Platform Description N/A

export map

Use this command to define the policy rule of exporting extended community attribute from local VRF to remote VPN route.

export map *routemap-name*

no export map *routemap-name*

Parameter Description	Parameter	Description
	routemap-name	Associated route map policy rule

Defaults No policy rule of exporting extended community attribute is defined by default.

Command Mode VPN configuration mode

Usage Guide Use this command to more precisely control the extended group attribute of an exported route. You are allowed to add or modify the extended community attribute defined by the **route-target export** command. The route map associated with this command supports only two rules: match IP address and set extcommunity.

Configuration Examples The following example configures a policy associated with rma on VPNA for exporting the extended group attribute.

```
Ruijie(config)# ip vrf VPNA
Ruijie(config-vrf)# export map rma
```

Related Commands	Command	Description
	route-target	Defines the policy for importing and exporting RTs for the VRF.

Platform Description N/A

extcommunity-type

Use this command to configure router-id or route-type of the OSPF instance associated with the VRF.

Use the **no** form of this command to restore to the default value.

extcommunity-type {**router-id** {**0107|8001**} **| route-type** {**0306|8000**}}

no extcommunity-type {**router-id | route-type** }

Parameter Description

Parameter	Description
router-id {0107|8001}	Sets the router-id of the OSPF instance. The value can be 0107 or 8001.
route-type {0306|8000}	Sets the route-type of the OSPF instance. The value can be 0306 or 8000.

Defaults The router-id is 0107 and the route-type is 0306 by default.

Command Mode OSPF Router mode

Usage Guide The command is valid only for the OSPF instance associated with the VRF, and not valid for the global VRF instance.

When the OSPF route of the VRF forms the VPN route, the extended community attribute of the VPN route carries the router-id information of the OSPF instance. The router-id field of the extended community attribute can be set to 0x0107 or 0x8001 by running the **extcommunity-type router-id** command.

When the OSPF route of the VRF forms the VPN route, the extended community attribute of the VPN route carries the route-type information of the OSPF instance. The route-type field of the extended community attribute can be set to 0x0306 or 0x8000 by running the **extcommunity-type route-type** command.

Configuration Examples The following example sets the router-id of the OSPF instance to 8001.

```
Ruijie(config)# router ospf 10 vrf vpn1
Ruijie(config-router)# extcommunity-type router-id 8001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

import map

Use this command to define the policy rule of importing remote VPN routes to local VRF.

import map *routemap-name*

no import map *routemap-name*

Parameter Description

Parameter	Description
routemap-name	Associated route map policy rule

Defaults No policy rule for importing remote VPN routes is defined by default.

Command Mode VPN configuration mode

Usage Guide Use this command to more precisely control the import of remote VPN routes to the local VRF. You can define an accurate rule as required in the associated route map. The rule defined by the **import map** command takes effect after the import of extended community attribute defined in the VRF. That is, the rule defined by this command filters the received remote VPN routes only when they match the extended community attribute defined by the **route-target import** command in the VRF. The route map associated with this command supports only two rules: match IP address and match extcommunity.

Configuration Examples The following example configures a import policy associated with rma on VPNA.

```
Ruijie(config)# ip vrf VPNA
Ruijie(config-vrf)# import map rma
```

Related Commands

Command	Description
route-target	Defines the policy for importing and exporting RTs for the VRF.

Platform Description N/A

ip extcommunity-list

Use this command to define the extended community list referenced by the route map, which is used to control the filtering of VPN routes in BGP/MPLS VPN applications.
Use the **no** form of this command to delete the extended community list.
ip extcommunity-list {*expanded-list* **| expanded** *list-name* **} {permit | deny}** *[regular-expression]*
ip extcommunity-list {*standard-list* **| standard** *list-name* **} {permit | deny} [rt** *value***] [soo** *value***]**
no ip extcommunity-list {*expanded-list* **| expanded** *list-name* **|** *standard-list* **| standard** *list-name* **}**
Use the following command to define the extended community list created by name.
Use the **no** form of this command to delete the extended community list.
ip extcommunity-list {*expanded-list* **| expanded** *list-name* **|** *standard-list* **| standard** *list-name* **}**
no ip extcommunity-list {*expanded-list* **| expanded** *list-name* **|** *standard-list* **| standard** *list-name***}**
Commands in expanded ip extcommunity-list configuration mode include:

[*sequence-number***]deny** *regular-expression*

[*sequence-number***] permit** *regular-expression*

exit

no [*sequence-number***]deny** *regular-expression*

no [*sequence-number***] permit** *regular-expression*

exit

Commands in standard ip extcommunity-list configuration mode include:

[*sequence-number***] deny {[rt** *value*] [**soo** *value*]**}**

[*sequence-number***] permit {[rt** *value*] [**soo** *value*]**}**

exit

no [*sequence-number***] deny {[rt** *value*] [**soo** *value*]**}**

no [*sequence-number***] permit {[rt** *value*] [**soo** *value*]**}**

exit

Parameter Description

Parameter	Description
expanded-list	Identifies the extended extcommunity list. It is in the range from 100 to 199. An extcommunity list can contain multiple rules.
standard-list	Identifies the standard extcommunity list. It is in the range from 1 to 99. An extcommunity list can contain multiple rules.
expanded *list-name*	Name of the extended extcommunity list, with a length of no more than 32 characters. This parameter allows you to enter extended community list configuration mode.
standard *list-name*	Name of the standard extcommunity list, with a length of no more than 32 characters. This parameter allows you to enter standard community list configuration mode.
permit	Defines an extcommunity permit rule.
deny	Defines an extcommunity deny rule.
regular-expression	(optional) Template to match extcommunity.
sequence-number	(Optional) Sequence number of a rule in the range from 1 to 2147483647. If this parameter is not specified, by default, when a rule is added, its sequence nubmer automatically increases by 10 starting from 10.
rt	(Optional) Sets the RT. This parameter can be used only for standard extcommunity configuration.
soo	(Optional) Sets the SOO. This parameter can be used only for standard extcommunity configuration.
value	Value of the extended extcommunity (extend_community_value). The extend_community_value may be in any of the following formats: ■ as_num:nn as_num is the public autonomous system number (a two-byte AS). nn is defined by the user, with a range from 0 to 4294967295.

	■ ip_addr:nn ip_addr must be the global IP address. nn is defined by the user, with a range from 0 to 65535. ■ as4_num:nn as4_num is the public autonomous system number (a four-byte AS). nn is defined by the user, with a range from 1 to 65535.  Note In 10.4(3) or later version, four-byte AS numbers are supported. That is, the new AS number is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format.

Defaults No extended community list is deifned by default.

Command Mode Global configuration mode or ip extcommunity-list configuration mode

Use this command to create an extcommunity rule list that contains multiple extcommunity values. This rule list is mainly applied by the match extcommunity rule of route map to match the extended community of BGP routes for route filtering.

For the definition of extended extcommunity, the rules of regular-expression are described as follows:

Symbol	Description
.	Matches any single character.
*****	Matches zero or any sequence in the character string.
+	Matches one or any sequence in the character string.
?	Matches zero or one symbol in the character string.
^	Matches the starting of the character string.
$	Matches the ending of the character string.
_	Matches the comma, bracket, starting and ending of the character string, and space.
[ ]	Matches the single character in a certain range.

Configuration Examples The following example defines an ip extcommunity-list.

```
Ruijie(config)# ip extcommunity-list 1 permit rt 100: 1
Ruijie(config)# ip extcommunity-list standard aaa permit rt
100: 2
Ruijie(config)# ip extcommunity-list expanded ext1 permit 200: [0~9][0~9]
The following example displays the use of ip extcommunity.
Ruijie(config)# route-map rt_in_filter
Ruijie(config-route-map)# match extcommunity 1
Ruijie(config-route-map)# match extcommunity ext1
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family vpn
```

```
Ruijie(config-router-af)#neighbor 3.3.3.3 send-community extended
Ruijie(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in
```

Related Commands	Command	Description
	match extcommunity	Matches the specific extcommunity attribute.

Platform Description N/A

ip route static inter-vrf

Use this command to enable the static inter-vrf route.
Use the **no** form of this command to disable the static inter-vrf route.
ip route static inter-vrf
no ip route static inter-vrf

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The static inter-vrf route is enabled by default.

Command Mode Global configuration mode

Usage Guide If you run the no ip route static inter-vrf command, the statically configured inter-vrf route will not take effect. If an active static inter-vrf route already exists, and you configure it again, information similar to the following will be printed to prompt you to delete the static inter-vrf route.
*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.*

Configuration Examples

```
Ruijie(config)# no ip route static inter-vrf
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ip route vrf

Use this command to create a static route entry for the VFR.
Use the **no** form of this command to delete the entry.

ip route vrf *vrf_name ip_addr mask* { *nexthop-address* | *interface-name* [*nexthop-address*] } [**enable|disable**] [**global**] [**permanent**] [tag *tag*] [weight *preference*]
no ip route vrf *vrf_name ip_addr mask* { *nexthop-address* | *interface-name* [*nexthop-address*] } [**enable|disable**] [**global**] [**permanent**] [tag *tag*] [weight *preference*]

Parameter Description

Parameter	Description
vrf-name	Name of the VRF
ip-addr	Prefix of the destination address of the route
mask	Mask of the prefix of the destination address
interface-name	Outgoing interface of the destination address
nexthop-address	Next hop of the destination address
global	Indicates that the next hop belongs to the global VRF.
enable	Activates the next hop of the configured route.
disable	Do not activate the next hop of the configured route.
permanent	The route will not be deleted even when the interface is shut down.
tag *tag*	Sets the tag of the route.
weight *preference*	Sets the weight of the route.

Defaults No static route is configured by default.

Command Mode Global configuration mode

Usage Guide The outgoing interface can be specified to an interface bound to another vrf so as to configure the static inter-VRF route. If the **global** parameter is configured, it is considered as the route of the global vrf. However, if the interface and **global** parameter are configured at the same time, and the interface is not within the global vrf, the vrf where the interface locates will be taken as the standard.


Note

The inter-vrf route that is configured to cross the global vrf by specifying the **global** parameter is not limited by the **no ip route static inter-vrf** command.

Configuration Examples

```
Ruijie(config)# ip route vrf vrf1 10.10.10.0 255.255.255.0 gi3/1 192.168.18.1
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

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	Name of the VRF

Defaults No vrf is defined by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# ip vrf vrf1
```

Related Commands

Command	Description
ip vrf forwarding	Binds the VRF with an interface.
show ip vrf	Displays the configuration of the VRF.
rd	Configures the RD for the VRF.
route-target	Configures the RT attribute for the VRF.

Platform Description N/A

ip vrf forwarding

Use this command to bind the VRF with an interface.

Use the **no** form of this command to remove the binding.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf_name*

Parameter Description

Parameter	Description
vrf-name	Name of the VRF

Defaults The VRF is not bound with any interface by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# int eth1
Ruijie(config-if)# ip vrf forwarding vrf1
```

Related Commands

Command	Description
ip vrf	Creates a VRF instance.
show ip vrf	Displays the configuration of the VRF.

Platform Description N/A

ipv6 route

Use this command to configure an IPv6 static route. Use the **no** form of this command to remove the configuration.

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface-id* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] [**weight** *number*]

no ipv6 route [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface-id* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*]

Parameter description

Parameter	Description
vrf-name	Specifies a VRF.
ipv6-prefix	Specifies an IPv6 prefix.
prefix-length	Specifies the prefix lengh.
ipv6-address	Specifies an IPv6 address.
interface-id	Specifies an interface.
vrf-name1	Specifies the VRF of the next hop.
default	The next hop is global.

distance	(Optional) Specifies the administrative distance of a staitc route.
number	(Optional)Specifies the weight value of a static route, in the range from 1 to 32.

Defaults N/A

Command mode Global configuration mode

Usage guidelines


Caution

If the destination IP address or the next hop address is the local address of the link, the outbound interface must be specified. If the destination IP address is the local address of the link and the next hop address must be a local address of the link, the destination IP address and the next hop address of the route cannot be multicast addresses. If the next hop address and the outbound interface are both specified, the outbound interface of the directly connected route for the next hop must be consistent with the configured outbound interface.


Caution

When the IPv6 address family is deleted from a multi-protocol VRF, the routing VRF or the netxt hop VRF will be deleted.


Caution

If an IPv6 static route is configured with an interface ID and next hop VRF, the VRF bound with the interface will not take effect if not consistent with the next hop VRF.

Examples The following example configures a global IPv6 route.

```
Ruijie(config)# ipv6 route 2001::/64 vlan 1 2005::1
```

The following example configures an IPv6 route from VRF1 to VRF2.

```
Ruijie(config)# vrf definition vrf1
Ruijie(config-vrf)# address-family ipv6
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config)# vrf definition vrf2
Ruijie(config-vrf)# address-family ipv6
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config-vrf)# ipv6 route vrf vrf1 2001::/64 1000::1 nexthop-vrf vrf2
```

The following example configures an IPv6 route from a VRF to the globe.

```
Ruijie(config)# vrf definition vrf1
Ruijie(config-vrf)# address-family ipv6
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config-vrf)# interface tunnel 1
```

```
Ruijie(config-if)# ipv6 address 1000::1/64
Ruijie(config-if)# tunnel mode ipv6ip
Ruijie(config-if)# tunnel source 1.1.1.1
Ruijie(config-if)# tunnel destination 1.1.1.2
Ruijie(config-if)# ipv6 route vrf vrf1 2000::/64 tunnel 1
```

Related commands	**Command**	**Description**
	N/A	N/A
Platform description	N/A	

match extcommunity

Use this command to define the rule of matching the extended community of BGP in route map configuration mode.

Use the **no** form of this command to remove 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	Identies the standard extcommunity list. It is in the range from 1 to 99. An extcommunity list can contain multiple extcommunity values.
standard-list-name	Name of the standard extcommunity list. An extcommunity list can contain multiple extcommunity values.
expanded-list-num	Identifies the extended extcommunity list. It is in the range from 100 to 199. An extcommunity list can contain multiple extcommunity values.
expanded-list-name	Name of the extended extcommunity list. An extcommunity list can contain multiple extcommunity values.

Defaults No match rule is deifned in the associated route map policy by default.

Command Mode Route map configuratin mode

Usage Guide The route map that contains the conditions for matching the extended community mainly applies in the following scenarios:

- For the route map associated by the **import map** command, it uses the RT attribute to filter the routes imported into the VRF.

- For the route map associated by the **neighbor route-map in** and **neighbor route-map out** commands, this command is executed in BGP VPNv4 address family configuration mode. The route map uses the RT attribute to filter the VPNv4 routes received from or sent to the BGP peer.

Configuration Examples

The following example defines two extended communities.

```
Ruijie(config)# ip extcommunity-list 1 permit rt 100: 1
Ruijie(config)# ip extcommunity-list 1 permit rt 100:2
```

The following example defines the match rule in the route map.

```
Ruijie(config)# route-map rt
Ruijie(config-route-map)# match extcommunity 1
```

The following exampel uses 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 Commands

Command	Description
ip extcommunity-list	Creates an extended community list.
show ip extcommunity-list	Displays the extended community list.

Platform Description

N/A

match mpls-label

Use this command to receive only the routes that contain the matching label from the BGP peer.

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

match mpls-label

no match mpls-label

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, if no match rule is deifned in the associated route map policy, the action of matching the MPLS label is not performed.

Command Mode

Route map configuratin mode

Usage Guide This command applies only to the route map associated by the **neighbor route-map in** command. It is used to manage only the incoming routes received from the BGP peer. If the rules defined in the route map do not contain the configuration of this command, routes are permitted as long as they meet the match rules defined in the route map, regardless of whether they carry the label.


Caution

This command is valid only for IPv4 routes carrying the label. It is not valid for VPNv4 routes.

Configuration Examples The following example creates a route map. In this example, a route is accepted only when it meets the following conditions:

The route prefix matches the rule defined in ACL 1.

The route contains the MPLS label.

```
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 Commands

Command	Description
neighbor send-label	Enables the exchange of routes carrying the MPLS label between BGP peers.
neighbor route-map out	Controls the routes sent to the BGP peer.
neighbor route-map in	Controls the routes received from the BGP peer.
set mpls-label	Assigns the MPLS label to routes that meet the filtering conditions defined in the route map.

Platform Description N/A

maximum routes

Use this command to set the maximum number of routes allowed in the VRF.

Use the **no** form of this command to cancel the setting.

maximum routes *limit* {*warn-threshold* **| warning-only**}

no maximum routes

Parameter Description

Parameter	Description
limit	Limits the number of routes. The routes that exceed the limit will not be written into the core route table. It is in the range from 1 to 4294967295.
warn-threshold	Threshold at which the warning is printed. The warning will be printed when this threshold is reached. The threshold is in the range from 1 to 100.

warning-only	When the configured limit is reached, the warning is printed, but routes are still allowed to be added to the core route table.

Defaults N/A

Command Mode VRF configuration mode

Usage Guide Use this command to limit the number of routes allowed in the VRF. If you only want the warning to be printed when the limit is reached, use the **warning-only** parameter.

Configuration Examples

```
Ruijie(config)# ip vrf vrf1
Ruijie(config-vrf)# rd 200:1
Ruijie(config-vrf)# maximum routes 1000 warning-only
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

neighbor activate

Use this command to activate the neighbor or the peer group in current address mode.
Use the **no** form of this command to restore to the default value.
neighbor {*peer-address* | *peer-group-name*} **activate**
no neighbor {*peer-address* | *peer-group-name*} **activate**

Parameter Description

Parameter	Description
peer-address	Specifies the address of the peer. This address may be the IPv4 or IPv6 address.
peer-group-name	Specifies the name of the peer group. The peer group name cannot exceed 32 characters.

Defaults The neighbor or the peer group is activated by default in the IPv4 address family.

Command Mode BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv6 address family configuration mode, BGP IPv4 VRF configuration mode, and BGP VPNv4 address family configuration mode

Usage Guide For the IPv4 address family, this function is enabled by default. For other address family types, you need to run this command for route information exchange.

Configuration Examples

```
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 peer of the BGP.

Platform Description N/A

neighbor allowas-in

Use this command to enable the PE to receive messages with AS numbers duplicated with its AS number during PE configuration.
Use the **no** form of this command to cancel the 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	Specifies the address of the peer.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.
number	Number of times deplicated AS numbers are allowed. It is in the range from 1 to 10. The default value is 3.

Defaults The allowas-in 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 configuration mode, and BGP VPNv4 address family configuration mode

Usage Guide The typical application is in the spoke-hub model. Run this command on the PE so that the PE can receive and send the address prefix that has been announced. Configure two VRFs on the PE. Set one of them to receive the route information of all PEs and to announce the received route information to the CE. Set the other VRF to receive the route information announced by the CE and to announce the received route information to all the PEs.
You can use this command on the IBGP peer or the EBGP peer.

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router)# address-family ipv4 vrf vpn1
Ruijie(config-router-af)# neighbor 10.0.0.1 allowas-in
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the peer of the BGP.

Platform Description N/A

neighbor as-override

Use this command to configure the PE to override the AS number of a site.

Use the **no** form of this command to restore the default value.

neighbor {*peer-address* | *peer-group-name*} **as-override**

no neighbor {*peer-address* | *peer-group-name*} **as-override**

Parameter Description

Parameter	Description
peer-address	Specifies the address of the peer.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.

Defaults The as-override function is disabled by default.

Command Mode BGP IPv4 VRF address family configuration mode

Usage Guide Normally, the BGP protocol will not receive route information with the AS number the same as the local AS number. Use this command to override the AS number so that the BGP protocol can receive the route information from the same AS number.

In the VPN, the most typical application lies in that two CE ends have the same AS number. Normally, these two CEs cannot receive information from each other. Execution of this command on the PE enables the PE to override the AS number of the CE so that the CE of the other end can receive the route information.

The as-override function can only set for the EBGP peer.

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 100
Ruijie(config-router)# address-family ipv4 vrf vpn
```

```
Ruijie(config-router-af)# neighbor 10.0.0.1 as-override
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the peer of the BGP.

Platform Description N/A

neighbor description

Use this command to add description for the specified peer (group).
Use the **no** form of this command to cancel the configuration.
neighbor {*peer-address* | *peer-group-name*} **description** *text*
no neighbor {*peer-address* | *peer-group-name*} **description**

Parameter Description

Parameter	Description
peer-address	Specifies the address of the peer.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.
text	Text used to describe the peer (group). The text can contain a maximum of 80 characters.

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 configuration mode, and BGP VPNv4 address family configuration mode

Usage Guide Use this command to add description for the peer (group). The description can help us better remember the characteristics and features of this peer (group).

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# neighbor 10.1.1.1 remote-as 80
Ruijie(config-router)# neighbor 10.1.1.1 description xyz.com
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the peer (group) of the BGP.

Platform Description N/A

neighbor next-hop-self

Use this command to modify the next hop to itself when sending routes to the peer (group).
Use the **no** form of this command to cancel the configuration.
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	Specifies the address of the peer.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.
next-hop-self	Modifies the next hop to itself when sending routes to the BGP peer.

Defaults The next hop is not modified by default when routes are sent to the IBGP peer.

Command Mode BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv6 address family configuration mode, BGP IPv4 VRF configuration mode, and BGP VPNv4 address family configuration mode

Usage Guide Use this command to modify the next hop to itself when sending routes to the peer (group).
In the inter-domain VPN OptionB solution, use this command in BGP VPN address configuration mode to modify the next hop.
This command is invalid if the neighbor is the route reflector client.

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# address-family vpnv4
Ruijie(config-router-af)# neighbor 10.1.1.1 next-hop-self
```

Related Commands

Command	Description
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the peer (group) of the BGP.

Platform Description N/A

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 cancel the configuration.
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	Specifies the address of the peer.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.
next-hop-unchanged	Maintains the next hop when sending routes to the BGP peer (group).

Defaults The next hop is modified by default when routes are sent to the EBGP peer.

Command Mode BGP configuration mode, BGP IPv4 address family configuration mode, and BGP VPN address family mode

Usage Guide In the inter-domain VPN OptionC (Multihop MP-EBGP) solution, you can set a route reflector in each AS to reduce the connections between PEs of inter-domain VPN. The route reflectors in different ASs set up Multihop MP-EBGP connections to exhcnage VPN routes. By default, the route reflector changes the next hop to itself when sending routes to the EBGP peer. Consequently, when PEs in other ASs receive the VPN routes, they consider the next hop of the VPN routes to be the route reflector. In this way, all inter-domain VPN traffic passes through the route reflector. This is not the optimal forwarding path and imposes higher demand on the forwarding performance of RR. To avoid this circumstance, when the route reflector establishes inter-domain Multihop MP-EBGP connections, run the **neighbor next-hop-unchanged** command in VPNv4 address family mode to maintain the next hop of VPNv4 routes sent to the BGP peer.

Configuration Examples

```
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 peer (group) of the BGP.

Platform Description N/A

neighbor remote-as

Use this command to configure the peer (group) of the BGP.
Use the **no** form of this command to delete the configured peer (group).
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	Specifies the address of the peer, which may be the IPv4 or IPv6 address.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.
as-number	AS number of the BGP peer (group). It is in the range from 1 to 65535.  Note In 10.4(3) or later version, four-byte AS numbers are supported. That is, the new AS number is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format.

Defaults No BGP peer is configured by default.

Command Mode BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv6 address family configuration mode, BGP IPv4 VRF configuration mode, and BGP VPNv4 address family configuration mode

Usage Guide If you specify the BGP peer group, all members of the peer group will inherit the setting of this command.

Configuration Examples

```
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 N/A

neighbor send-label

Use this command to enable the exchange of IPv4 routes carrying the MPLS label with the specified peer (group).
Use the **no** form of this command to disable the funciton.
neighbor {*peer-address* | *peer-group-name*} **send-label**
no neighbor {*peer-address* | *peer-group-name*} **send-label**

Parameter Description

Parameter	Description
peer-address	Specifies the address of the peer.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot

	exceed 32 characters.
send-label	Sends IPv4 routes carrying the MPLS label to the BGP peer (group).

Defaults Routes carrying the MPLS label are not sent to the BGP peer by default.

Command Mode BGP configuration mode, BGP IPv4 address family configuration mode, and BGP IPv4 VRF address family configuration mode

Usage Guide Use this command to enable the exchange of IPv4 routes carrying the MPLS label with the specified peer. This command must be configured on the local rotuer and the adjacent router. If the BGP session has been set up, this configuration takes effect after the BGP session resets.


Caution

To enable distribution of labels for IPv4 routes on the IBGP session, use the **neighbor** *{peer-address|peer-group_name}* **update-source loopback** *id* command to set the the loopback address as the source address of the BGP session. Otherwise, this command cannot be configured. If you use the IP address of the direct interface as the source address, the LDP will distribute label-3 to its upstream devices for the connected P device considers the direct route to be the outgoing interface. In this way, the LSP tunnel is terminated on the P device, not the PE. Therefore, the loopback address (usually a 32-bit mask) must be used to identify the PE itself, to ensure that the outgoing interface of LSP is the PE. For a direct EBGP session, you do not need to bind the loopback address. Instead, you can use the IP address of the direct interface as the source address of the EBGP session. This is because, for the single-hop direct EBGP session that enables BGP routes (IPv4 routes or VPN routes) to carry with label, the MP-BGP automatically generates a host route with the length of a 32-bit mask to the outgoing interface (namely the EBGP neighbor address) to prevent LSP from being terminated in advance for the host address is aggregated by the direct route. In this case, the LDP will not send label-3 to its upstream through the host route of EBGP neighbor address because it does not consider itself to be the outgoing interface.

When you use BGP as the label distribution protocol, run the **label-switching** command to enable the label forwarding function on the interface on which MPLS messages need to be forwarded.

Configuration Examples The following example enables the exchange of IPv4 routes carrying the MPLS label with the peer 10.0.0.1.

```
Ruijie(config)# router bgp 65000
Ruijie(config-router)# neighbor 10.0.0.1 remote-as 65501
Ruijie(config-router)# neighbor 10.0.0.1 update-source loopback 0
Ruijie(config-router)# neighbor 10.0.0.1 send-label
```

Related

Command	Description

Commands		
	neighbor route-map in	Sets the policy of receiving routes from the peer.
	neighbor route-map out	Sets the policy of sending routes to the peer.
	label-switching	Enables the label forwarding function on the interface.
	match mpls-label	Matches the MPLS label defined in the route map.
	set mpls-label	Distributes the MPLS label to the routes matching the route map.

Platform Description N/A

neighbor shutdown

Use this command to disable the BGP connection established with the specified BGP peer.
Use the **no** form of this command to restart the BGP peer (group).

neighbor {*peer-address* | *peer-group-name*} **shutdown**
no neighbor {*peer-address* | *peer-group-nam*e} **shutdown**

Parameter Description

Parameter	Description
peer-address	Specifies the address of the peer, which may be the IPv4 or IPv6 address.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.

Defaults The neighbor shutdown 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 configuration mode, and BGP VPNv4 address family configuration mode

Usage Guide Use this command to disable the valid connection established with the specified peer (group) and delete all associated route information. The configuration information of this peer (group) is not deleted.
If you specify the BGP peer group, all members of the peer group will inherit the setting of this command. However, if you set this command for a certain member of the peer, this setting will override the peer group-based setting.

Configuration Examples

```
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 peer of the BGP.
show ip bgp summary	Displays the connection status of the BGP.

Platform Description N/A

neighbor soo

Use this command to configure the neighbor source site attribute value.

Use the **no** form of this command to cancel the neighbor source site attribute value.

neighbor {*peer-address* | *peer-group-name*} **soo** *soo-value*

no neighbor {*peer-address* | *peer-group-name*} **soo**

Parameter Description

Parameter	Description
peer-address	Specifies the address of the peer.
peer-group-name	Specifies the name of the peer group. The name of the peer group cannot exceed 32 characters.
soo-value	Value of soo. The soo-value may be in any of the following formats: ■ as-num:nn as-num is the public autonomous system number (a two-byte AS). nn is defined by the user, with a range from 0 to 4294967295. ■ ip-addr:nn ip_addr must be the global IP address. nn is defined by the user, with a range from 0 to 65535. ■ as4_num:nn as4_num is the public autonomous system number (a four-byte AS). nn is defined by the user, with a range from 1 to 65535.  Note In 10.4(3) or later version, four-byte AS numbers are supported. That is, the new AS number is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format.

Defaults The soo function is ndisabled by default.

Command Mode BGP IPv4 VRF address family configuration mode

Usage Guide In the CE dual-home model, use this command to prevent the route information sent from the CE to the PE being sent back to the CE.

Configuration Examples

```
Ruijie(config)# router bgp 65000
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 soo 100:100
```

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.

Platform Description N/A

neighbor tnl-policy

Use this command to configure a tunnel policy for VRF. Use the **no** form of this command to remove the configuration.

neighbor *ip-address* **tnl-policy** *policy-name*

no neighbor *ip-address* **tnl-policy**

Parameter description	Parameter	Description
	ip-address	Specifies the IP address of a BGP peer.
	policy-name	Specifies the tunnel policy name

Defaults VRF uses the tunnel selection policy by default.

Command mode VRF configuration mode/Multi-protocol VRF configuration mode

Usage guidelines One BGP peer in a VRF can be configured with only one tunnel policy.

Examples The following example

```
Ruijie(config)# ip vrf vrf1
Ruijie(config-vrf)# neighbor 2.2.2.2 tnl-policy tnl-pol
```

Related commands	Command	Description
	N/A	N/A
Platform description	N/A	

rd

Use this command to define the RD value of the VRF.

rd *rd-value*

Parameter Description

Parameter	Description
rd_value	The RD value. The rd_value may be in any of the following formats: ■ as_num:nn as_num is the public autonomous system number (a two-byte AS). nn is defined by the user, with a range from 0 to 4294967295. ■ ip_addr:nn ip_addr must be the global IP address. nn is defined by the user, with a range from 0 to 65535. ■ as4_num:nn as4_num is the public autonomous system number (a four-byte AS). nn is defined by the user, with a range from 1 to 65535.  Note In 10.4(3) or later version, four-byte AS numbers are supported. That is, the new AS number is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format.

Defaults No RD value is configured by default.

Command Mode VRF configuration mode

Usage Guide If you have defined a VRF and configured an RD value for it, the RD value cannot be modified. If modifying the RD value is required, first delete the VRF, configure it again, and then set a new RD value for it.

A VRF can have only one RD value.

Note

In 10.4(3) or later version, RD attribute configuration is added for AS4. That is, it is allowed to configure the RD attribute for 4-byte ASs. The RD attribute of 4-byte ASs is in the format of AS4:NN. AS4 can be a decimal value or in dot format. AS4 is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format. NN is in the range from 1 to 65535.


Caution

For AS numbers in the range from 1 to 65535, they are stored as 2-byte ASs. This is because they are displayed the same, regardless of whether they are expressed as decimal values or in dot format.

Configuration Examples

```
Ruijie(config)# ip vrf vrf1
Ruijie (config-vrf)# rd 100:1
```

Related Commands

Command	Description
ip vrf	Creates a VRF instance.
show ip vrf	Displays the configuration information of the VRF.

Platform Description N/A

recursive-route lookup lsp

Use this command to enable the function of resolving the next hop of the BGP route to the LSP tunnel.

Use the **no** form of this command disables the function.

recursive-route lookup lsp

no recursive-route lookup lsp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function of resolving the next hop of the BGP route to the LSP tunnel is disabled by default.

Command Mode Global configuration mode

Usage Guide By default, the next hop of the BGP route without a label is not resolved to the LSP tunnel. In a CSC application scenario, for the model where level 2 carriers provide Internet services based on the IP core, the next hop of the BGP route must be resolved to the LSP tunnel on the CSC CE. Use this command to enable this function.

Configuration Examples The following example enables the function of resolving the next hop of the BGP route to the LSP tunnel.

```
Ruijie(config)# recursive-route lookup lsp
```

Related

Command	Description

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

redistribute

Use this command to enable the redistribution between the route information of other route protocols and BGP.

Use the **no** form of this command to disable the function and delete its parameter configuration.

redistribute *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]

no redistribute *protocol-type* [**route-map** *map-tag*] [**metric**]

Parameter Description

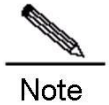
Parameter	Description
protocol-type	Type of the source protocol of the redistributed route. The following types are available: connected, static, and rip.
route-map *map-tag*	Name of the associated route-map. No route-map is associated by default.
metric *metric-value*	Default metric value of the configured redistribution route. This parameter is not set by default.

Defaults The redistribution function is disabled by default.

Command Mode BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv6 address family configuration mode, and BGP IPv4 VRF configuration mode

Usage Guide

If a device supports multiple routing protocols, the coordination between these protocols is important. To run multiple routing protocols at the same time, a device must be able to redistribute information among the protocols. This is applicable to all IP routing protocols.


Note

If the **no** form of this command is executed with parameters specified, and there are corresponding parameter configurations, it will cancel the configuration of corresponding parameters. If no parameter is specified, the **no** form of this command will disable the redistribution function.


Caution

For the metric value of the route, it will apply the route-map for processing based on the original value. If it is processed in the route-map, the value after the route-map processing will be used. If this value is not set in the route-map, but the metric option is

configured, the value configured by the metric option will be used. If both the route-map and the metric option are not configured, the redistributed value will be used.

Configuration Examples

```
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 protocols	Displays the global configuration information of the routing protocols.

Platform Description N/A

redistribute ospf

Use this command to enable the redistribution between the route information of the OSPF routing protocol and BGP.

Use the **no** form of this command to disable the function and delete its parameter configuration.

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**] **[match {internal|external [1|2]|nssa-external [1|2]}]**

Parameter Description

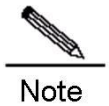
Parameter	Description
process-id	Process ID of the redistributed OSPF protocol
route-map *map-tag*	Name of the associated route-map. No route-map is associated by default.
metric *metric-value*	Default metric value of the configured redistribution route. This parameter is not set by default.
match	Sets the matched subtype of the OSPF route.
internal	Internal subtype of the OSPF route. It is the default configuration of match item for the redistributed OSPF route.
external [1|2]	External type of the OSPF route. You can specify it as type 1 or type 2. If it is not specified,type 1 and type 2 are included.
nssa-external [1|2]	Nssa-external type of the OSPF route. You can specify it as type 1 or type 2. If it is not specified, type 1 and type 2 are included.

Defaults Redistribution of the OSPF route is disabled by default.

Command Mode BGP configuration mode, BGP IPv4 address family configuration mode, BGP IPv6 address family configuration mode, and BGP IPv4 VRF configuration mode

Usage Guide

If a device supports multiple routing protocols, the coordination between these protocols is important. To run multiple routing protocols at the same time, a device must be able to redistribute information among these protocols.


Note

If the **no** form of this command is executed with parameters specified, and there are corresponding parameter configurations, it will cancel the configuration of corresponding parameters. If no parameter is specified, the **no** form of this command will disable the redistrution function. When all of the route subtypes are deleted, the default route type is used.


Caution

The filtering rule of the OSPF route is as follows: First the OSPF route type is filtered according to the configured match option, and then filtering is performed according to the route-map rule. For the metric value of the route, the route-map processing is performed based on the redistributed metric value. If it is processed in the route-map, the value after the route-map processing will be used. If it is not processed in the route-map, but the metric option is configured, the value configured by the metric option will be used. If both the route-map and the metric option are not configured, the redistributed value will be used.

Configuration Examples

```
Ruijie(config-router)# redistribute ospf 2 route-map static-rmap
Ruijie(config-router)# no redistribute ospf 4 match external route-map
ospf-rmap
Ruijie(config-router)# no redistribute ospf 78
```

Related Commands

Command	Description
show ip protocols	Displays the global configuration information of the routing protocols.

Platform Description

N/A

route-target

Use this command to define the Route-Target (RT) attribute of a VRF.
Use the **no** form of this command to cancel the RT attribute of a VRF.
route-target {**import | export | both**} *rt-value*
no route-target {**import|export|both**} *rt_value*

Parameter Description

Parameter	Description
import	Sets the import RT value for the VRF.

export	Sets the export RT value for the VRF.
both	Sets the import and export RT values for the VRF.
rt_value	The rt_value may be in any of the following formats: ■ as_num:nn as_num is the public autonomous system number (a two-byte AS). nn is defined by the user, with a range from 0 to 4294967295. ■ ip_addr:nn ip_addr must be the global IP address. nn is defined by the user, with a range from 0 to 65535. ■ as4_num:nn as4_num is the public autonomous system number (a four-byte AS). nn is defined by the user, with a range from 1 to 65535.  Note In 10.4(3) or later version, four-byte AS numbers are supported. That is, the new AS number is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format.

Defaults The RT value is not defined by default.

Command Mode VRF configuration mode

Usage Guide You can configure multiple import and export RT attribute values for a VRF.

Configuration Examples

```
Ruijie(config)# ip vrf vrf1
Ruijie(config-vrf)# route-target import 100:1
Ruijie(config-vrf)# route-target export 100:2
Ruijie(config-vrf)# route-target both 100:4
```

Related Commands

Command	Description
ip vrf	Creates a VRF instance.

Platform Description N/A

set extcommunity

Use this command in route map configuration mode to set the extended community value for routes matching the route map when sending route update messages to the BGP peer.

set extcommunity {**rt** *extended-community-value* **[additive] | soo** *extended-community-value*}

no set extcommunity {rt | soo}

Parameter Description

Parameter	Description
rt	Sets the RT value.
soo	Sets the SOO value.
additive	(Optional) Adds new RT attribute to the RT list, insteading of replacing any existing RT attributes.
extended-community-value	Extended community value. You can set multiple RT values separated by space, but only one SOO value. The extend_community_value may be in any of the following formats: ■ as_num:nn as_num is the public autonomous system number (a two-byte AS). nn is defined by the user, with a range from 0 to 4294967295. ■ ip_addr:nn ip_addr must be the global IP address. nn is defined by the user, with a range from 0 to 65535. ■ as4_num:nn as4_num is the public autonomous system number (a four-byte AS). nn is defined by the user, with a range from 1 to 65535. Note: In 10.4(3) or later version, four-byte AS numbers are supported. That is, the new AS number is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format.

Defaults This rule is not defined in the associated route map policy by default. Without additive, this command will replace all RT lists.

Command Mode Route map configuratin mode

Usage Guide This command applies to the following scenarios:

4) Route map associated by the **export map** command, which controls the extended community of VPN routes based on policy.

5) Route map associated by the **neighbor route-map {in|out}** command configured in BGP VPNv4 address family mode, which modifies received and sent VPNv4 routes.

If the **additive** parameter is not specified, the **set extcommunity rt** command replaces the original RT value with the set one. If the **additive** parameter is specified, this command adds the new RT value to the existing RT list.

If no SOO attribute is available in the existing extended community attribute list of BGP route, the **set extcommunity soo** command adds the SOO attribute. If an SOO attribute is available, this command replaces the original SOO value with the set one.


Note

In 10.4(3) or later version, configuration of extended community attribute is added for AS4. That is, it is allowed to configure the extended community attribute for 4-byte ASs. The extended community attribute of 4-byte ASs is in the format of AS4:NN. AS4 can be a decimal value or in dot format. AS4 is in the range from 1 to 4294967295, which is 1..65535.65535 in dot format. NN is in the range from 1 to 65535


Caution

For AS numbers in the range from 1 to 65535, they are stored as 2-byte ASs. This is because they are displayed the same, regardless of whether they are expressed as decimal values or in dot format.

Configuration Examples

```
Ruijie(config)# route-map set-rt
Ruijie(config-route-map)# set extcommunity rt 100:1 200:1
Ruijie(config-route-map)# exit
Ruijie(config)# ip vrf vrf1
Ruijie(config-vrf)# export map set-rt
```

Related Commands

Command	Description
match extcommunity	Matches the specified extended community attribute.

Platform Description N/A

set mpls-label

Use this command in route map configuration mode to assign the MPLS label to the routes matching the route map when sending route update messages to the BGP peer.

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

set mpls-label

no set mpls-label

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, if this rule is not defined in the associated route map policy, the IPv4 routes sent to the BGP peer do not carry the MPLS label.

Command Mode Route map configuratin mode

Usage Guide This command applies only to the route map associated by the **neighbor route-map out** command, which is used to filter only the outbounding routes sent to the BGP peer.

This command takes effect in the route map only after the **neighbor send-label** command is executed to enable exchange of the routes carrying the MPLS label between the BGP peers. Othewise, the command distributes the routes matching the route map without the label. On the other hand, if you use the **neighbor send-label** command to enable exchange of the routes carrying the MPLS label between the BGP peers, but does not configure the **set mpls-label** command for the associated route map, the IPv4 routes matching the route map are distributed without carrying the MPLS label.

Configuration Examples The following example creates a route map, which distributes the MPLS label to the route with prefix 1.1.1.1/32, distributes common IPv4 route updates without the MPLS label to the route with prefix 1.1.1.2/32, but does not distribute route updates to the neighbor for routes that do not match ACL1 and ACL2.

```
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-std-nacl) # exit
Ruijie (config)# route-map out-as permit 20
Ruijie (config-route-map)# match ip address acl
```

Related Commands

Command	Description
neighbor send-label	Enables exchange of routes carrying the MPLS label between the BGP peers.
neighbor route-map out	Controls the routes sent to the BGP peer.
match mpls-label	Receives only the routes carrying the MPLS label from the BGP peer.
show ip bgp labels	Displays the routes carrying the MPLS label that the BGP learns and sends.

Platform Description N/A

show bgp ipv4 unicast labels

Use this command to display the routes carrying the MPLS label that the BGP learns and sends.

show bgp ipv4 unicast labels

Parameter

Parameter	Description

Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IP routes carrying the MPLS label. To display the VPN routes carrying the MPLS label, run the show bgp vpnv4 unicast command.

Configuration Examples The following example displays information about label distribution for IPv4 routes using BGP on ASBR.

```
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	Next hop of the route
In label	Label that the local router assigns (if available)
Out label	Label learned from the next hop router of the route (if available)

Related Commands

Command	Description
neighbor send-label	Enables exchange of routes carrying the MPLS label between the BGP peers.
show bgp vpnv4 unicast	Displays the label informaiton of VPN routes.

Platform Description N/A

show bgp ipv6 unicast labels

Use this command to display the routes carrying the MPLS label that the BGP learns and sends.

show bgp ipv6 unicast labels

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IPv6 routes carrying the MPLS label. To display the VPN routes carrying the MPLS label, run the **show bgp vpnv6 unicast** command.

Configuration Examples The following example displays information about label distribution for IPv6 routes using BGP on 6PE.

```
Ruijie# show bgp ipv6 unicast labels
BGP table version is 2, local router ID is 111.1.1.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop       In Label/Out Label
*>i193::/64         ::ffff:2.2.2.2     nolabel/21
*>i666::/64         ::ffff:2.2.2.2     nolabel/20
*> 888::1/128       ::               1536/nolabel
*>i2001::/64        ::ffff:3.3.3.3     nolabel/19
*>i2005::/64        ::ffff:3.3.3.3     nolabel/18
*> 3000::/64        ::               1541/nolabel
```

Field	Description
Network	Route prefix
Nexthop	Next hop of the route
In label	Label that the local router assigns (if available)
Out label	Label learned from the next hop router of the route (if available)

Related Commands

Command	Description
neighbor send-label	Enables exchange of routes carrying the MPLS label between the BGP peers.
show bgp vpnv6 unicast	Displays the label informaiton of VPN routes.

Platform Description N/A

show bgp vpnv4 unicast

Use this command to display the VPN route information.

show bgp vpnv4 unicast all [*network* | **neighbor** [*peer-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	Displays the prefix of the specified destination network.

neighbor [*peer-address*]	Displays the neighbor information of the specified VPN.
summary	Displays the state of the BGP peer.
label	Displays the label information of the route.
all	Displays the VPN route information of all VRFs.
vrf_name	Displays the VPN route information of the specified VRF.
rd_value	Displays the VPN route information of the specified RD value.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the VPN route information. In the BGP/MPLS VPN application environment, the routes of BGP VRF instances are elected and imported by MP-BGP. Therefore, the **show bgp vpnv4 unicast vrf** command displays only elected routes. To view detailed MP-BGP route information, use the **show bgp vpnv4 unicast all** command.

Configuration Examples

```
Ruijie# show bgp vpnv4 unicast all
Network        Nexthop     Metric  Localprf           Path
Route Distinguisher : 100:2
*>i 192.168.0.1/32  192.168.0.2  0      100    10 ?
*>i 192.168.1.0/32  192.168.0.2    0      100     ?
Route Distinguisher : 100:30
*>i 192.168.0.1/32  192.168.0.2  0      100    10 ?
*> 192.168.4.0  192.168.4.1      0            20 ?
* 192.168.4.0    0.0.0.0           0      32768     ?
```

Field	Description
*	The route is valid.
s (lowercase)	The route is suppressed by the aggregate route.
S (uppercase)	The route is an old entry.
>	The route is preferentially elected.
i	The route is learned from IBGP.
Nexthop	Next-hop information of the route
Metric	Metric value of the route
Localprf	Local priority attribute of the route
Path	AS-path included in the route
i	The ORINGIN attribute of the route is IGP.
e	The ORINGIN attribute of the route is EGP.
?	The ORINGIN attribute of the route is the one other than IGP and EGP (for example, BGP route added by redistribution).

```
Ruijie# show bgp vpnv4 unicast vrf vpn1 summary
BGP router identifier 192.168.0.4 , local AS num 100
BGP  VRF vrf1 Route  Distinguisher : 100 : 30
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries
Neibhbor   V   AS   MsgRcvd  Msgsend TblVer  IntQ
OutQ   Up/Down  State/PfxRcd
192.168.4.1 4  20    15      16    1       0    0
00:10:36    3
Total number of neighbors 1
```

Field	Description
num BGP AS-PATH entries	Number of BGP AS-Path entries
num BGP community entries	Number of BGP community entries
V	BGP version
AS	AS number of the BGP peer
MsgRcvd	Total number of BGP messages received from the BGP peer
Msgsend	Total number of BGP messages sent to the BGP peer
TblVer	Routing table version of the BGP VPN address family. The routing table version will be updated each time all the VPN routes are sent to the BGP peer. The routing table version will not be updated untill new VPN routes need to be sent to the BGP peer.
Up/Down	It the BGP peer has been set up, this field indicates the duration from the BGP peer was set up till now. If this field is displayed as "never", it indicates that the BGP peer is not set up.
State/PfxRcd	If the BGP peer has been set up, this field indicates the number of VPN routes received from the BGP peer. If the BGP peer is not set up,this field indicates the state of the BGP peer.

```
Ruijie#show bgp vpnv4 unicast all 172.168.0.1
BGP routing table entry for 100:1:172.168.0.1/32, version 24
Paths: (1 available, best #1, table aa)
 Not advertised to any peer
 Local
   1.1.1.1 (metric 2) from 1.1.1.1 (1.1.1.1)
     Origin incomplete, metric 2, localpref 100, valid, internal, best
     Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x040404040200 OSPF
ROUTER ID:172.168.0.2:0 OSPF RT:0.0.0.0:2:0
     mpls labels in/out nolabel/21
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show bgp vpnv6 unicast

Use this command to display the VPNv6 route information.

show bgp vpnv6 unicast all [*network* | **neighbor** [*peer-address*] | **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	Displays the prefix of the specified destination network.
neighbor [*peer-address*]	Displays the neighbor information of the specified VPN.
summary	Displays the state of the BGP peer.
label	Displays the label information of the route.
all	Displays the VPN route information of all VRFs.
vrf_name	Displays the VPN route information of the specified VRF.
rd_value	Displays the VPN route information of the specified RD value.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the VPN route information. In the BGP/MPLS VPN application environment, the routes of BGP VRF instances are elected and imported by MP-BGP. Therefore, the **show bgp vpnv6 unicast vrf** command displays only elected routes. To view detailed MP-BGP route information, use the **show bgp vpnv6 unicast all** command.

Configuration Examples

```
Ruijie# show bgp vpnv6 unicast all
Network        Nexthop     Metric  Localprf           Path
Route Distinguisher :  100: 2
*>i 10::/64        192.168.0.2    0      100     10 ?
*>i 10:1::/64      192.168.0.2    0      100      ?
Route Distinguisher : 100:30
*>i 10:2::/64      192.168.0.2    0      100     10 ?
*>  10:3::/64      192.168.4.1    0             20 ?
```

```
*   10:4::/64       0.0.0.0       0       32768     ?
```

Field	Description
*	The route is valid.
s (lowercase)	The route is suppressed by the aggregate route.
S (uppercase)	The route is an old entry.
>	The route is preferentially elected.
i	The route is learned from IBGP.
Nexthop	Next-hop information of the route
Metric	Metric value of the route
Localprf	Local priority attribute of the route
Path	AS-path included in the route
i	The ORINGIN attribute of the route is IGP.
e	The ORINGIN attribute of the route is EGP.
?	The ORINGIN attribute of the route is the one other than IGP and EGP (for example, BGP route added by redistribution).

```
Ruijie# show bgp vpnv4 unicast vrf vpn1 summary
BGP router identifier 192.168.0.4 , local AS num 100
BGP  VRF vrf1 Route  Distinguisher : 100 : 30
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries
Neibhbor   V   AS   MsgRcvd  Msgsend TblVer  IntQ
OutQ   Up/Down  State/PfxRcd
192.168.4.1 4  20    15      16    1       0    0
00:10:36    3
Total number of neighbors 1
```

Field	Description
num BGP AS-PATH entries	Number of BGP AS-Path entries
num BGP community entries	Number of BGP community entries
V	BGP version
AS	AS number of the BGP peer
MsgRcvd	Total number of BGP messages received from the BGP peer
Msgsend	Total number of BGP messages sent to the BGP peer
TblVer	Routing table version of the BGP VPN address family. The routing table version will be updated each time all the VPN routes are sent to the BGP peer. The routing table version will not be updated untill new VPN routes need to be sent to the BGP peer.
Up/Down	It the BGP peer has been set up, this field indicates the duration from the BGP peer was set up till now. If this field is displayed as "never", it indicates that the BGP peer is not set up.

State/PfxRcd	If the BGP peer has been set up, this field indicates the number of VPN routes received from the BGP peer. If the BGP peer is not set up,this field indicates the state of the BGP peer.

```
Ruijie#show bgp vpnv4 unicast all 172.168.0.1
BGP routing table entry for 100:1:172.168.0.1/32, version 24
Paths: (1 available, best #1, table aa)
 Not advertised to any peer
 Local
   1.1.1.1 (metric 2) from 1.1.1.1 (1.1.1.1)
     Origin incomplete, metric 2, localpref 100, valid, internal, best
     Extended Community: RT:100:1 OSPF DOMAIN ID:0x0005:0x040404040200 OSPF
ROUTER ID:172.168.0.2:0 OSPF RT:0.0.0.0:2:0
     mpls labels in/out nolabel/21
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip extcommunity-list

Use this command to display the configuration of the extended community list.

show ip extcommunity-list [*extcommunity-list-num*| *extcommunity-list-name*]

Parameter Description

Parameter	Description
extcommunity-list-num	Identifies the standard or extended extcommunity list. It is in the range from 1 to 199.
extcommunity-list-name	Name of the standard or extended extcommunity list

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration 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 Commands

Command	Description
ip extcommunity-list	Creates the extended community list.
match extcommunity	Matches the specified extended community attribute.
set extcommunity	Sets the specified extended community attribute.

Platform Description N/A

show ip ospf sham-links

Use this command to display the OSPF sham link information.

show ip ospf *[process-id]* **sham-links [area** *area-id***]**

Parameter Description

Parameter	Description
process-id	Process ID of the OSPF
area *area-id*	OSPF area-id of the sham link. It can be a decimal integer ranging from 0 to 4294967295 or an IP address.

Defaults N/A

Command Mode Privileged user mode

Usage Guide Use this command to display the sham link information of the OSPF instance.

Configuration Examples

```
ruijie#show ip ospf sham-links
Sham Link SLINK1 to address 8.8.8.8 is up
  Area 0.0.0.0 source address 7.7.7.7, Cost: 10
  Output interface is GigabitEthernet 0/8
  Nexthop address 192.168.1.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
    Adjacency state Full
```

Related

Command	Description

Commands	N/A	N/A

Platform Description N/A

show ip vrf

Use this command to display the configured VRF information.

show ip vrf [**brief** | **detail** | **interfaces**] [*vrf-name*]

Parameter Description

Parameter	Description
brief	(Optional) Displays brief information of the VRF and its interface.
detail	(Optional) Displays detailed information of the VRF and its interface.
interfaces	(Optional) Displays detailed information of the VRF and its interface.
vrf-name	(Optional) Specifies the VRF.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the VRF name is specified, this command displayes information of the specified VRF. If no VRF name is specified, this command displays the information of all VRFs.

Configuration Examples

```
Ruijie# show ip vrf detail vrf1
VRF pe1;default RD : 100:2
Interfaces:
Eth0
Export VPN route-target communities:
RT :100:30
No import VPN route-target community
No import route-map
```

Related Commands

Command	Description
ip vrf	Creates a VRF instance.
rd	Configures the RD value.
route-target	Configures the RT value.
ip vrf forwarding	Binds the VRF with an interface.

Platform N/A

Description

show vrf

Use the following command to view brief information of a VRF (a single-protocol IPv4 VRF or a multi-protocol VRF).

show vrf [brief] [*vrf-name*]

Use the following command to view brief information of a VRF (which can be a single-protocol IPv4 VRF) configured with an IPv4 address family.

show vrf ipv4 [*vrf-name*]

Use the following command to view brief information of a VRF configured with an IPv6 address family.

show vrf ipv6 [*vrf-name*]

Use the following command to view detailed information of a VRF (a single-protocol IPv4 VRF or a multi-protocol VRF).

show vrf detail [*vrf-name*]

Parameter Description

Parameter	Description
vrf-name	Name of the VRF

Defaults N/A

Command Mode Privileged user mode

Usage Guide N/A

Configuration Examples The following example displays brief information of all VRFs.

```
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
```

Related Commands

Command	Description
ip vrf	Defines a single-protocol IPv4 VRF.
vrf definition	Defines a multi-protocol VRF.

Platform Description N/A

vrf definition

Use this command to create a multi-protocol VRF.

vrf definition *vrf-name*

Parameter Description

Parameter	Description
vrf-name	Name of the VRF. It is a string of up to 31 characters.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Do not use this command to edit a single-protocol VRF. Do not use the **ip vrf** command (single-protocol VRF configuration command) to edit a multi-protocol VRF either.

Configuration Examples The following example creates multi-protocol VRF vrf1.

```
Ruijie(config)#vrf definition vrf1
Ruijie(config-vrf)#
```

Related Commands

Command	Description
description	Configures the descriptor.
address-family	Configures an IPv4 or IPv6 address family for the multi-protocol VRF.
exit-address-family	Exits VRF address family configuration mode.
vrf forwarding	Binds a network interface to the multi-protocol VRF.

Platform Description N/A

vrf forwarding

Use this command to bind a network interface to the specified multi-protocol VRF.

vrf forwarding *vrf-name*

Parameter Description

Parameter	Description
vrf-name	Name of the VRF. The specified VRF must be a multi-protocol VRF. It cannot be a single-protocol VRF that only supports IPv4.

Defaults A network interface is not bound to any VRF by default.

Command Mode Interface configuration mode

Usage Guide Do not use this command to bind a network interface to a single-protocol VRF. Do not use the **ip vrf**

forwarding command to bind a network interface to a multi-protocol VRF either.

Do not bind the interface to a multi-protocol VRF that is not configured with any address family.

To bind a network interface to a multi-protocol VRF, delete existing IPv4 addresses, VRRP IPv4 addresses, IPv6 addresses, and VRRP IPv6 addresses, and disable the IPv6 protocol on the interface.

When binding a network interface to a multi-protocol VRF, note the following:

- If no IPv4 address family is configured for the VRF, do not configure IPv4 addresses and VRRP IPv4 addresses for the VRF. You must configure an IPv4 address family for the VRF before configuring IPv4 addresses and VRRP IPv4 addresses for it.
- If no IPv6 address family is configured for the VRF, do not configure IPv6 addresses and VRRP IPv6 addresses for the VRF. You must configure an IPv6 address family for the VRF before configuring IPv6 addresses and VRRP IPv6 addresses for it.

If you delete the IPv4 address family of a multi-protocol VRF, all IPv4 addresses and VRRP IPv4 addresses on the network interface bound to this VRF, as well as IPv4 static routes of the route VRF and IPv4 static routes whose next hop is this VRF will be deleted. Similarly, if you delete the IPv6 address family of a multi-protocol VRF, all IPv6 addresses and VRRP IPv6 addresses on the network interface bound to this VRF, as well as IPv6 static routes of the route VRF and IPv6 static routes whose next hop is this VRF will be deleted, and the IPv6 protocol on the interface will be disabled.

Configuration Examples

The following example binds interface VLAN 1 to multi-protocol 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	Creates a multi-protocol VRF.

Platform Description

N/A

L2VPN Commands

address-family l2vpn

Use this command to enter l2vpn address family configuration mode to configure l2vpn information exchange of the BGP neighbor.
Use the **no** form of this command to exit l2vpn address family configuration mode.
adress-family l2vpn {vpls|vpws}
no adress-family l2vpn {vpls|vpws}

Parameter Description

Parameter	Description
vpls	L2VPN vpls address family
vpws	L2VPN vpws address family

Defaults The l2vpn address family is not defined by default.

Command Mode BGP configuration mode

Usage Guide Use the **address-family l2vpn vpls** command to allow l2vpn vpls information exchange between PEs and enter VPLS address family configuration mode. Use the **address-family l2vpn vpws** command to allow l2vpn vpws information exchange between PEs and enter VPWS address family configuration mode. Use the **exit-address-family** command to exit address-family l2vpn configuration mode.

Configuration Examples
```
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family l2vpn vpls
Ruijie(config-router)# address-family l2vpn vpws
```

Related Commands

Command	Description
neighbor activate	Activates an address family.
exit-address-family	Exits this mode.

Platform Description N/A

clear bgp l2vpn

Use this command to reset the l2vpn address family information in the BGP neighbor session.

clear bgp l2vpn {vpls|vpws} {*|as number|*neighbor address*} **[soft] [in [prefix-filter] | out]]**

Parameter Description

Parameter	Description
vpls	Resets the created BGP session with the VPLS capability.
vpws	Resets the created BGP session with the VPWS capability.
*****	Resets all the created BGP sessions with the VPLS or VPWS capability.
neighbor address	Resets the created BGP session of the specified neighbor with the VPLS or VPWS capability.
as number	Autonomous system number of the BGP peer (group) in the range from 1 to 65535 In 10.4(3) or later versions, 4-byte AS number is supported, that is, the new AS number range is from 1 to 4294967295, which is 1..65535.65535 in dot mode.
in	Soft resets the received routing information.
out	Soft resets the distributed routing information.
soft	Soft resets routing information received from or sent to the specified peer.
soft in	Soft resets the received routing information.
soft out	Soft resets the distributed routing information.
prefix-filter	(Optional) Currently, this parameter is not effective and is only for compatibility with the configuration of peer vendors.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If this command is used without the IP address of a certain peer being specified, all BGP VPLS or VPWS neighbor sessions will be reset.

Configuration Examples

```
Ruijie#clear bgp l2vpn vpls *
Ruijie#clear bgp l2vpn vpws *
```

Related Commands

Command	Description
show bgp l2vpn	Displays the Kompella vfi instance information.

Platform Description N/A

clear bgp l2vpn dampening

Use this command to reset the l2vpn route oscillation information in the specified BGP neighbor session.

clear bgp l2vpn {vpls|vpws} dampening [*ve-id:offset*]

Parameter Description

Parameter	Description
vpls	Resets the BGP session of VPLS.
vpws	Resets the BGP session of VPWS.
dampening	Route oscillation
ve_id:offset	Displays the vfi instance information of the specified ve_id:offset.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to reset the l2vpn route oscillation information in the BGP neighbor session.

Configuration Examples

```
Ruijie#clear bgp l2vpn vpls dampening
Ruijie#clear bgp l2vpn vpws dampening
```

Related Commands

Command	Description
clear bgp l2vpn	Resets the l2vpn address family information in the BGP neighbor session.
show bgp l2vpn	Displays the l2vpn vfi instance information.

Platform Description N/A

clear bgp l2vpn external

Use this command to reset all l2vpn EBGP connections.

clear bgp l2vpn {vpls|vpws} external[soft] [in | out]]

Parameter Description

Parameter	Description
vpls	Resets the EBGP session of VPLS.
vpws	Resets the EBGP session of VPLS.
external	Specifies EBGP.
in	Soft resets the received routing information.
out	Soft resets the distributed routing information.

soft	Soft resets the routing information received from or sent 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 Use this command to reset all I2vpn EBGP connections and all I2vpn EBGP neighbor sessions.

Configuration Examples

```
Ruijie#clear bgp l2vpn vpls external
Ruijie#clear bgp l2vpn vpws external
```

Related Commands

Command	Description
clear bgp l2vpn	Resets the I2vpn address family information in the BGP neighbor session.
show bgp l2vpn	Displays the I2vpn vfi instance information.

Platform Description N/A

clear bgp l2vpn flap-statistics

Use this command to reset the I2vpn route oscillation statistics in the specified BGP neighbor session.

clear bgp l2vpn {vpls|vpws} flap-statistics [*ve-id:offset*]

Parameter Description

Parameter	Description
vpls	Resets the EBGP session of VPLS.
vpws	Resets the EBGP session of VPWS.
flap-statistics	Statistics of route oscillation
ve_id:offset	Displays the vfi instance information of the specified ve_id:offset.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to reset the I2vpn route oscillation statistics in the specified BGP neighbor session.

Configuration Examples

```
Ruijie#clear bgp l2vpn vpls flap-statistics
Ruijie#clear bgp l2vpn vpws flap-statistics
```

Related Commands

Command	Description
clear bgp l2vpn	Resets the I2vpn address family information in the BGP neighbor session.
show bgp l2vpn	Displays the I2vpn vfi instance information.

Platform Description N/A

clear bgp l2vpn peer-group

Use this command to reset the BGP sessions with all members in a peer group.

clear bgp l2vpn {vpls|vpws} peer-group *name* **[soft] [in | out]]**

Parameter Description

Parameter	Description
vpls	Resets the BGP session of VPLS.
vpws	Resets the BGP session of VPWS.
peer-group	Peer group
name	Peer group name
in	Soft resets the received routing information.
out	Soft resets the distributed routing information.
soft	Soft resets the routing information received from or sent 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 Use this command to reset the BGP sessions with all members in a peer group.

Configuration Examples

```
Ruijie#clear bgp l2vpn vpls peer-groute group1
Ruijie#clear bgp l2vpn vpws peer-groute group2
```

Related Commands

Command	Description
clear bgp l2vpn	Resets the I2vpn address family information in the BGP neighbor session.

show bgp l2vpn	Displays the l2vpn vfi instance information.

Platform Description N/A

clear l2 vfi

Use this command to clear all the MAC addresses that are learnt from PW from the specified local or remote VPLS instance.

clear l2 vfi *name* **mac-address** {**remote|local** [*mac-address*]}

Parameter Description

Parameter	Description
name	Name of the VPLS instance
remote	Sends the MAC address cancel message carrying zero MAC address to all the neighbors of the Hub PW of the specific VPLS instance through the LDP.
local *mac-address*	Clears all MAC addresses from the specified VPLS instance or the specified dynamic MAC addresses.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The **clear l2 vfi mac-address local** command clears all dynamic MAC addresses from the local VPLS instance. It is valid only for dynamically learnt MAC addresses.

The **remote** parameter in this command is valid only for VPLS of the LDP signaling. It triggers the LDP to send a MAC withdraw message to a remote PE. Upon receiving the MAC withdraw message, the remote PE will clear all MAC addresses (excluding the PW). The **remote** parameter in this command is invalid for VPLS of the BGP signaling.

Configuration Examples The following example clears a local dynamic MAC address in vfi1.

```
Ruijie# clear l2 vfi vfi1 mac-address local 001a.a915.3218
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

description

Use this command to set the description of the l2vpn vfi instance.

Use the **no** form of this command to remove the description.

description *desc*

no description

Parameter Description

Parameter	Description
desc	Description of the l2vpn vfi instance, a string of up to 63 characters

Defaults No description is defined for the l2vpn vfi instance by default.

Command Mode VFI configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config-vfi)#description vfi-description
```

Related Commands

Command	Description
show mpls vfi	Displays information of the l2vpn vfi instance .

Platform Description N/A

encapsulation

Use this command to specify the PW encapsulation mode for the l2vpn vfi instance.

Use the **no** form of this command to restore to the default value ethernet.

encapsulation mpls [**ethernet** | **ethernetvlan|ppp|hdlc| ip-interworking**]

no encapsulation mpls

Parameter Description

Parameter	Description
mpls	Encapsulation type
ethernet	The PW type for VPWS is specified as ethernet. The PW encapsulation mode for VPLS is raw mode.
ethernetvlan	The PW type for VPWS is specified as ethernetvlan. The PW encapsulation mode for VPLS is tag mode.
ppp	Specifies the PW type as ppp, which is valid only for VPWS.
hdlc	Specifies the PW type as hdlc, which is valid only for VPWS.

ip-interworking	Specifies the PW type as the heterogeneous media interworking mode, which is valid only for VPWS.

Defaults Kompella I2vpn uses ethernet by default.

Command Mode VFI configuration mode

Usage Guide This command is valid only for the I2vpn realized in Kompella mode. It is invalid for the VPLS realized in Martini mode. Only ethernet and ethernetvlan are valid for the VPLS in Kompella mode to specify VPLS PW encapsulation mode (raw or tag).

For the VPWS in Kompella mode, all types are valid to specify the VPWS PW type for BGP signaling negotiation.

Note the following:

For the VPLS in Kompella mode, the PW encapsulation mode of one VPLS on different PEs should be the same; otherwise the asymmetry of the VLAN tag handling may lead to normal forwarding. It is recommended that the PW encapsulation mode be set to raw (ethernet) if every PE of a VPLS adopts Ethernet interface access, and the PW encapsulation mode be set to tag (ethernetvlan) if every PE of a VPLS adopts subinterface access or hybrid interface access.

For the VPLS in Kompella mode, PW type on the two ends of a PW must be the same; otherwise BGP signaling cannot negotiate to establish the PW.

If the VFI instance has already bound with the interface, it is not allowed to modify the encapsulation mode. The VFI must be unbound from the interface before modifying the encapsulation mode.

Configuration Examples Example 1:

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vpls-name1 vpnid 10 autodiscovery
Ruijie(config-vfi)# encapsulation mpls ethernet
```

Example 2:

```
Ruijie(config)# l2 vfi vpls-name2 vpnid 20 point-to-point
Ruijie(config-vfi)# encapsulation mpls ethernet
```

Related Commands

Command	Description
signal	Configures the PW signaling of I2vpn vfi.

Platform Description N/A

exit-site-mode

Use this command to exit config-vfi-site configuration mode.

exit-site-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults -

Command Mode config-vfi-site configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie (config-vfi-site)# exit-site-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ignore match l2-extcommunity

Use this command to determine whether the PW created in Kompella mode matches the layer 2 extended community attribute.
Use the **no** form of this command to restore to the default configuration.
ignore match l2-extcommunity
no ignore match l2-extcommunity

Parameter Description

Parameter	Description
N/A	N/A

Defaults Lay 2 extended community attribute must be matched by default when the PW is created between PEs in Kompella mode.

Command Mode VFI configuration mode

Usage Guide This command is valid only for the VPLS and VPWS implemented in Kompella mode. It is invalid for the VPLS implemented in Martini mode.
During the creation of PW in Kompella I2vpn mode, the negotiation packet contains the I2vpn encapsulation type and MTU information by using the BGP extended community attribute. By default, PW can be set up between two vfi instances only when the encapsulation type and MTU of these two vfi instances are the same. Use this command to allow PW establishment even when the

encapsulation type and MTU do not match between two vfi instances.

Configuration Examples The following example configures the Kompella VPLS instance not to match layer 2 extended community attribute.

```
Ruijie(config)# l2 vfi vpls-name vpnid 10 autodiscovery
Ruijie(config-vfi)# ignore match l2-extcommunity
```

The following example configures the Kompella VPWS instance not to match layer 2 extended community attribute.

```
Ruijie(config)# l2 vfi vpls-name vpnid 10 point-to-point
Ruijie(config-vfi)# ignore match l2-extcommunity
```

Related Commands

Command	Description
signal	Configures PW signaling.

Platform Description N/A

l2 vfi

Use this command to create an l2vpn vfi instance or enter VFI configuration mode.
Use the **no** form of this command to remove the specified l2vpn vfi instance.
l2 vfi *name* [**vpnid** <1- 2147483647> [**manual| autodiscovery|point-to-point**]]
no l2 vfi *name*

Parameter Description

Parameter	Description
name	Name of the l2vpn vfi instance in a string of up to 31 characters
<1-2147483647>	VPLS instance ID
manual	Implements the VPLS in Martini mode, which requires the user to create the PW by configuring the VPLS neighbor manually.
autodiscovery	Implements the VPLS in Kompella mode, which creates the PW by autodiscovery.
point-to-point	Implements the VPWS in Kompella mode, which auto-discovers the specified PE device in the VFI instance.

Defaults VPLS is implemented in Martini mode by default.

Command Mode Global configuration mode

Usage Guide Names of l2vpn vfi instances are mapped to vpnids one by one. When this command is executed without the **vpnid** *id* parameter being specified, VFI configuration mode is entered. In this case, the **name** parameter can only be set to an existing l2vpn vfi instance; otherwise, an error message will be displayed.

If this command is executed with parameters (including the parameters indicating name, id, and configuration mode) being specified the same as the original setting, VFI configuration mode is entered.

Auto-discovery is effective only after the l2vpn vpls or l2vpn vpws address family has been activated in BGP configuration mode.

VPLS is implemented in Kompella mode only when the keyword **autodiscovery** is specified. VPWS is implemented in Kompella mode only when the keyword **point-to-point** is specified. If no keyword is specified or the keyword **manual** is specified, VPLS is implemented in Martini mode.

Once Kompella or Martini mode is selected to implement l2vpn vfi, the implementation mode cannot be modified. If the implementation mode needs to be modified, remove the instance and reconfigure it. An example is as follows: VPLS is configured to be implemented in Kompella mode, but you want to change the implementation mode to Martini. You have to remove the VPLS instance, then create the VPLS instance again and configure VPLS to be implemented in Martini mode.

For VPLS or VPWS implemented in Kompella mode, PW can be established for the corresponding VPLS or VPWS instance only when the rd, site-id, and route-target have been configured and the interface has been bound.

For VPLS implemented in Martini mode, PW can be established for the corresponding VPLS instance only when the interface has been bound or a Spoke VC neighbor has been created.

Configuration Examples

The following example creates a VPLS instance implemented in Martini mode.

```
Ruijie(config)# l2 vfi vfi_1 vpnid 1
```

or

```
Ruijie(config)#l2 vfi vfi_1 vpnid 1 manual
```

The following example creates a VPLS instance implemented in Kompella mode.

```
Ruijie(config)#l2 vfi vfi_1 vpnid 1 autodiscovery
```

The following example creates a VPWS instance implemented in Kompella mode.

```
Ruijie(config)#l2 vfi vfi_2 vpnid 1 point-to-point
```

The following example enters VFI configuration mode to modify the configuration of the specified vfi instance.

```
Ruijie (config)# l2 vfi vfi_1
```

The following example removes the specified vfi instance.

```
Ruijie (config)# no l2 vfi vfi_1
```

Related Commands

Command	Description
description	Sets the description of a vfi instance.
mtu	Sets the MTU of a vfi instance.
address-family l2vpn	Configures the l2vpn address family.
neighbor active	Activates the neighbor to support the exchange of l2vpn address family information.
show mpls vfi	Displays the l2vpnvfi instance information.

Platform Description

N/A

l2 vfi switching

Use this command to create a switching-VFI instance or enter the Switching-VFI mode. Use the **no** form of this command to remove the configuration.

l2 vfi *name* **switching**

no l2 vfi *name* **switching**

Parameter description

Parameter	Description
name	Sets the switching-VFI instance name
no	Removes the switching-VFI instance

Defaults N/A

Command mode Global configuration mode

Usage guidelines The local switching-VFI can share the same name with the local L2VPN VFI.

Examples The following example creates a switching-VFI instance.

```
Ruijie(config)#l2 vfi ms-pw switching
Ruijie(config-vfi)#
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

l2 vfi tunnel-protocol stp

Use this command to enable transparent transmission of STP packets on the interface bound with the VPLS instance.

l2 vfi tunnel-protocol stp

no l2 vfi tunnel-protocol stp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The BPDU packet of STP is not transparently transmitted by default.

Command Mode Interface configuration mode

Usage Guide Usually, a BPDU packet does not carry the VLAN Tag. If CE access is based on the Trunk interface or subinterface, and transparent transmission of BPDU packets needs to be enabled on the access interface, the BPDU packets sent by the CE must carry the VLAN Tag that can be identified by the corresponding VPLS instance. Otherwise, the BPDU packets cannot be transparently transmitted within this VPLS instance.
This command does not depend on whether the interface has been bound with the VPLS instance.

Configuration Examples

```
Ruijie(config-if)#l2 vfi tunnel-protocol stp
```

Related Commands

Command	Description
xconnect vfi	Enables the Martini VPLS service on the specified interface.

Platform Description N/A

label-saving

Use this command to configure label-saving mode for Kompella VPWS. Label-saving mode is not supported by default.
label-saving enable
no label-saving enable

Parameter Description

Parameter	Description
enable	Enable label-saving.

Defaults Label-saving mode is not supported by default.

Command Mode VFI configuration mode

Usage Guide This command is valid only for the VPWS implemented in Kompella mode. It is invalid for the VPLS instance.
After label-saving mode is enabled, Kompella VPWS will set offset based on the configured remote site id and allocate a label on demand. The site range locally configured will become invalid.

Configuration Examples

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vpls-name vpnid 10 point-to-point
Ruijie(config-vfi)#label-saving enable
```

Related Commands

Command	Description
l2 vfi	Configures a VFI instance, which can be a VPLS instance or a Kompella VPWS instance.

Platform Description N/A

local-ce mac

Use this command to specify the static MAC address of CE.

Use the **no** form of this command to restore to the default value.

local-ce mac *mac*

no local-ce mac

Parameter Description

Parameter	Description
mac	During the heterogeneous media interworking, if the PE and CE use Ethernet lines for connections, the MAC address of the CE must be configured on the PE. If the MAC address of the CE is not configured, the destination MAC uses the broadcast address for encapsulation by default.

Defaults The broadcast address is not used to fill the destination MAC of the CE by default.

Command Mode vfi site configuration mode

Usage Guide For the VPWS service of the heterogeneous media interworking in Kompella mode, if the PE and CE connect to an Ethernet interface, the MAC address of the CE must be configured on the PE. If the MAC address is not configured, the destination MAC uses the broadcast address for encapsulation by default. This command is valid only for the VPWS of the heterogeneous media interworking. It is invalid for the VPWS of the homogeneous media interworking.

Configuration Examples

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vpls-name1 vpnid 10 point-to-point
Ruijie(config-vfi)# encapsulation mpls ip-interworking
Ruijie(config-vfi)# site-id 3 site-range 32
Ruijie(config-vfi-site)#xconnect interface gi 0/0 remote-ce-id 2
Ruijie(config-vfi-site)#local-ce mac 00d0.f810.1234
```

Related Commands

Command	Description
signal	Configures the PW signaling of I2vpn vfi.

Platform Description N/A

mac-address aging-time

Use this command to configure the MAC address aging time of the VPLS instance.
Use the **no** form of this command to restore to the default configuration.
mac-address aging-time *interval*
no mac-address aging-time

Parameter Description

Parameter	Description
aging-time *interval*	Configures the MAC address aging time of the VPLS instance. The aging time is in the range from 5 to 65536 seconds.

Defaults The default aging time of the VPLS instance is 300 seconds (5 minutes).

Command Mode VFI configuration mode

Usage Guide The aging time is valid only for MAC addresses dynamically learned. It is invalid for MAC addresses statically configured. The MAC addresses statically configured can be deleted only by static user configuration.
After the aging time is reset, the new aging time will be taken as the benchmark to update the aging time of all MAC entries of the VPLS instance. For example, if the aging time is changed from 5 minutes to 10 minutes, all MAC entries of the VPLS instance age after 10 minutes. If the aging time is changed from 10 minutes to 5 minutes, all MAC entries of the VPLS instance age after 5 minutes.

Configuration Examples The following example sets the aging time of the VPLS instance to 180 seconds (3 minutes).

```
Ruijie(config)#l2 vfi vfi_1 vpnid 1 manual
Ruijie(config-vfi)# mac-address aging-time 180
```

Related Commands

Command	Description
l2 vfi	Creates a vfi instance or enters VFI configuration mode. The **no** form of this command deletes the vfi instance.
show mpls vfi	Displays the I2vpn vfi instance information.

Platform Description N/A

mac-learning

Use this command to configure the MAC learning policy.

mac-learning [**ac | pw**] { **disable | enable** }

Parameter Description

Parameter	Description
ac	Learns the MAC address of the AC.
pw	Learns the MAC address of the PW.
enable	Enables MAC learning.
disable	Disables MAC learning.

Defaults The AC MAC address and the PW MAC address are learned by default.

Command Mode VFI configuration mode

Usage Guide If both **ac** and **pw** are not specified, AC MAC and PW MAC learning are enabled or disabled simultaneously. If a local PE serves as the UPE with a limited MAC capacity, it is recommended to disabled MAC learning on the UPE. If the UPE receives a packet from an AC and does not know its MAC address, the packet is sent to the NPE.

Configuration Examples The following example disables PW MAC learning.

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vfi_a vpnid 1
Ruijie(config-vfi)# mac-learning pw disable
```

Related Commands

Command	Description
l2 vfi	Creates a vfi instance or enters VFI configuration mode. The **no** form of this command deletes the vfi instance.
show mpls vfi	Displays the I2vpn vfi instance information.

Platform Description N/A

mac-limit

Use this command to configure MAC address learning limit rules of the VPLS instance.

Use the **no** form of this command to restore to the default value.

mac-limit [**action {discard|forward}**] [**alarm** {**disable|enable**}] [**maximum** *count*]

no mac-limit {**action|alarm |maximum**}

Parameter

Parameter	Description

Description

action	Forwards the packets with new source MAC addresses when the number of MAC addresses of the VPLS instance reaches the threshold.
discard	Discards the packets with new source MAC addresses when the number of MAC addresses of the VPLS instance reaches the threshold.
forward	Continues to forward the packets with new source MAC addresses when the number of MAC addresses of the VPLS instance reaches the threshold.
alarm	Determines whether to print the log information when the MAC capacity of the VPLS instance reaches the threshold or reduces below the threshold again.
disable	Log information is not printed when the MAC capacity of the VPLS instance reaches the threshold or reduces to less than 80% of the threshold again.
enable	Log information is printed when the MAC capacity of the VPLS instance reaches the threshold or reduces to less than 80% of the threshold again.
maximum *count*	Configures the threshold of the MAC addresses for the VPLS instance. The range is from 0 to 65536. The value 0 indicates that the MAC capacity of the VPLS instance is not limited.

Defaults The default threshold of the MAC addresses of the VPLS instance is 256.
By default, the packets with new source MAC addresses are discarded when the number of MAC addresses of the VPLS instance reaches the threshold.
By default, log information is not printed when the number of MAC addresses of the VPLS instance reaches the threshold or reduces to less than 80% of the threshold again.

Command Mode VFI configuration mode

Usage Guide The VPLS instance learns the source MAC addresses of the packets on both the PW and AC ends during forwarding. If the number of MAC addresses learned by the VPLS instance reaches the threshold configured for the VPLS instance, the VPLS instance does not learn new MAC addresses. You can run the **maximum** *count* command to set the threshold of MAC addresses of the VPLS instance to a larger value.
If the **maximum** *count* command is executed to change the threshold of MAC addresses of the VPLS instance to a smaller value, the dynamic MAC addresses that exceed the new threshold will age immediately. The new threshold of MAC addresses cannot be smaller than the number of static MAC addresses configured for the VPLS instance; otherwise, the configuration fails.
The **mac-limit action {discard|forward}** command determines whether to discard or forward the packets with new source MAC addresses after the number of MAC addresses learned by the VPLS instance reaches the threshold.
The **mac-limit action {discard|forward}** command determines whether to print log information for

users when the number of MAC addresses learned by the VPLS instance reaches the threshold or reduces below the threshold again. If the **mac-limit alarm enable** command is executed, log information is printed in one of the following cases:
The number of MAC addresses learned by the VPLS instance reaches the threshold configured for the VPLS instance.
The number of MAC addresses learned by the VPLS instance reached the threshold, but some MAC addresses are deleted due to MAC address aging or other reasons (such as command configuration), which causes the number of MAC addresses to reduce to less than 80% of the threshold for the first time.

Configuration Examples

```
Ruijie(config)#l2 vfi vfi_1 vpnid 1 manual
Ruijie(config-vfi)# mac-limit maximum 1024
```

Related Commands

Command	Description
l2 vfi	Creates a VPLS instance or enters VPLS mode. The **no** form of this command deletes the VPLS instance.
show mpls vfi	Displays the I2vpn vfi instance information.

Platform Description N/A

mac-withdraw

Use this command to enables a PE to forward the mac-withdraw message to neighbors. Use the **no** form of this command to remove the configuration.
mac-withdraw enable
no mac-withdraw enable

Parameter description

Parameter	Description
N/A	N/A

Defaults A PE does not forward the MAC-withdraw message to neighbors by default.

Command mode VFI mode

Usage guidelines After the local PE is enabled with mac-withdraw, if the PE receives a mac-withdraw message from the UPE, it forwards the message to the NPE. If the PE receives a mac-withdraw message from the NPE, it does not forward the message to the other PEs. If mac-withdraw is disabled on the local PE, the local PE does not forward forward the message to the other PEs.
After the PE receives the mac-withdraw message, all dynamic MAC addresses except the that of the peer PW will be deleted.

If you want to enable the local PE to serve as the message source, run the **clear l2 vfi** *name* **mac-address remote** message.

Examples The following example enables a VPLS intance with MAC-withdraw.

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vfi_a vpnid 1
Ruijie(config-vfi)# mac-withdraw enable
```

Related commands	**Command**	**Description**
	N/A	N/A
Platform description	N/A	

mpls static-l2vc

Use this command to configure the outgoing label and incoming label of the static PW. Use the **no** form of this command to remove the configuration.

mpls static-l2vc *ip-address vc-id* **out-label** *out-label-value* **in-label** *in-label-value*

no mpls static-l2vc *ip-address vc-id*

Parameter description	**Parameter**	**Description**
	ip-address	Specifies the peer IPv4 address of a static PW.
	vc-id	Specifies the PW ID of a static PW, in the range from 1 to 2147483647.
	out-label *out-label-value*	Specifies the outgoing label of a static PW, in the range from 16 to 1048575.
	in-label *in-label-value*	Specifies the incoming label of a static PW, in the range from 16 to 1023.

Defaults N/A

Command mode Global configuration mode

Usage guidelines Create a static PW before configuring the outgoing label and the incoming label.

PE devices on both ends need to create a static VC connection. The outgoing label and the incoming label of a static PW on one end correspond to the incoming label and the outgoing label of the static PW on the other end respectively.

Examples The following example sets the outgoing lable and the incoming lable of a static PW to 100.

```
Ruijie(config)#interface FastEthernet 0/2
```

```
Ruijie(config-if)#xconnect 1.1.1.1 1 encapsulation mpls manual
Ruijie(config-if)#exit
Ruijie(config)# mpls static-l2vc 1.1.1.1 1 out-label 100 in-label 100
```

Related commands	Command	Description
	N/A	N/A
Platform description	N/A	

mpls static vfi

Use this command to configure the static MAC address of the VPLS instance.
Use the **no** form of this command to delete the configured static MAC address.
mpls static vfi *name* **mac-address** *H.H.H* **{neighbor** *ip-address***|interface** *interface-name***}**
no mpls static vfi *name* **mac-address** *H.H.H* **{neighbor** *ip-address***|interface** *interface-name***}**

Parameter Description

Parameter	Description
name	Name of the VPLS instance
H.H.H	Static MAC address
neighbor *ip-address*	Address of the VPLS neighbor
interface *interface-name*	Interface of the VPLS AC end

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to configure the MAC address of the VPLS neighbor or the MAC address of the interface bound with VPLS.
After the static MAC address of the VPLS neighbor is configured, it is valid only when the PW corresponding to the VPLS neighbor is up.
When the static MAC address of the VPLS AC is configured, the interface must be bound with the VPLS instance. If the interface is not bound with the VPLS instance, the MAC address is invalid. If the interface was previously bound with the VPLS instance, but later the VPLS instance was unbound from the interface, the MAC address is also invalid.
The MAC entry learned dynamically is overwritten when the statically configured MAC address conflicts with and the dynamic MAC address.


Caution

The static MAC address that associates with the PW by configuring the neighbor address can function normally only in the following scenario: There is only one PW for the neighbor of the VPLS instance. If there are many PWs, the statically configured

MAC address is randomly bound with one PW, which may lead to incorrect forwarding.

Configuration Examples

The following example configures the MAC address of the VPLS neighbor.

```
Ruijie(config)# mpls static vfi vfi1 mac-address .a915.3218 neighbor .1
```

The following example configures the MAC address of the VPLS AC.

```
Ruijie(config)# mpls static vfi vfi1 mac-address 0022.7b15.3218 interface gi1/1
```

Related Commands

Command	Description
l2 vfi	Creates a vfi instance or enters VFI configuration mode. The **no** form of this command deletes the vfi instance.
show mpls vfi	Displays the I2vpn vfi instance information.

Platform Description

N/A

mtu

Use this command to configure the mtu of the vfi instance.

Use the **no** form of this command to restore to the default value.

mtu *mtu*

no mtu

Parameter Description

Parameter	Description
mtu	mtu value in the range of 46 to 1530

Defaults

The mtu of the vfi instance is 1500 by default.

Command Mode

VFI configuration mode

Usage Guide

The mtu of the vfi instance indicates the size (length after the MPLS label is encapsulated) of a packet that can be transmitted by the PW, that is, the length of the user layer-2 packet and PW encapsulation. By default, if the PW does not enable control word, and two labels are encapsulated, the length of the user Ethernet packet that can be transmitted is 1492 bytes, of which 8 bytes are the PW encapsulation (two labels).

The mtu of the vfi instance takes effect for all PWs of the vfi instance. That is, PWs use the mtu of the vfi instance for negotiation. By default, a PW cannot be established if the mtu cannot be negotiated to be consistent between the two ends of the PW.


Caution

If the mtu negotiated by the PW signaling protocol is modified, the mtu (usually the value

of PW mtu minus the label encapsulation) of the user service access interface must be adjusted. In addition, the mtu of the outgoing interface on the PW's public network side must be modified to be the same as the PW mtu for proper forwarding. You can run the **mtu** command to modify the mtu of the interface.

Configuration Examples

```
Ruijie(config-vfi)# mtu 1500
```

Related Commands

Command	Description
l2 vfi	Creates a vfi instance or enters vfi configuration mode. The **no** form of this command deletes the vfi instance.
mtu	Configures the mtu of the vfi instance.
show mpls vfi	Displays the l2vpn vfi instance information.

Platform Description N/A

neighbor activate

Use this command to activate the neighbor to support I2vpn address family.
Use the **no** form of this command to disable the activation.
neighbor {*ip-address* | *peer-group-name*} **activate**
no neighbor {*ip-address* | *peer-group-name*} **activate**

Parameter Description

Parameter	Description
ip-address	IP address
peer-group-name	Specifies the peer group name. The name cannot contain more than 32 characters.

Defaults The neighbor is deactivated by default.

Command Mode BGP I2vpn address family configuration mode

Usage Guide For the configuration of the I2vpn VPLS or VPWS address family, use this command to activate I2vpn information exchange through BGP.

Configuration Examples

```
Ruijie# config terminal
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family l2vpn vpls
Ruijie(config-router-af)# neighbor 10.10.10.1 activate
```

Related Commands

Command	Description
address-family	Enables the I2vpn address family.
router bgp	Enables the BGP protocol.
neighbor remote-as	Configures the BGP peer.

Platform Description N/A

neighbor(VPLS configuration mode)

Use this command to configure VPLS neighbors.

neighbor *ip-address* **encapsulation mpls** [**vc-id** *vc-id*] [**hub-vc** | **spoke-vc**] [**ethernet** | **ethernetvlan**]

no neighbor *ip-address* **encapsulation mpls**

Parameter Description

Parameter	Description
ip-address	LSR ID of the VPLS neighbor
vc-id *vc-id*	PW ID in the range from 1 to 2147483647. The VPN ID is used as the PW ID by default.
hub-vc	Specifies the PW as the hub PW.
spoke-vc	Specifies the PW as the spoke PW.
ethernet	Sets the PW type to ethernet.
ethernetvlan	Sets the PW type to ethernetvlan.

Defaults By default, the created PW is ethernet-type hub VC and its VC ID is the same as the VPN ID of the VPLS instance.

Command Mode VFI configuration mode

Usage Guide This command is valid only for VPLS implemented in Martini mode. It is invalid for VPLS implemented in Kompella mode.

PWs use PW IDs and LSR IDs of the PW peers as key. The PWs (including the PWs used by VPWS) must be globally unique.

To avoid loop, VPLS must use full interconnection networking mode. A PW connection must be set up between every two PEs. This PW connection is called Hub-VC. When this command is used for configuration of the same neighbor, the latest configuration overwrites the previous configuration. When U-PE accesses N-PE as a PW in the H-VPLS model, or a user accesses VPLS service as a PW in the basic VPLS model, the PW must be configured as a PW of the spoke-vc type (Spoke-PW) on the VPLS N-PE or VPLS-PE.

Caution

For either Spoke-VC or Hub-VC, the MTU and PW type must be configured the same on both ends; otherwise the PW cannot be up.

The PW type cannot be modified once the VPLS PW is configured. To modify the PW type, delete the VPLS PW and then configure another one.

Configuration Examples The following example creates a default PW, with VC-ID set to the VPN ID and PW type set to ethernet type Hub-VC.

```
Ruijie(config-vfi)#neighbor 2.2.2.2 encapsulation mpls
```

The following example creates an ethernetvlan-type spoke-VC with VC-ID of 100.

```
Ruijie(config-vfi)#neighbor 3.3.3.3 encapsulation mpls vc-id 100 spoke-vc ethernetvlan
```

Related Commands

Command	Description
l2 vfi	Creates a vfi instance or enters VFI configuration mode. The **no** form of this command deletes the vfi instance.
show mpls vfi	Displays the vfi instance information.

Platform Description N/A

neighbor (Switching-VFI mode)

Use this command to configure pseudo wires for a switching-VFI instance. Use the **no** form of this command to remove the configuration.

neighbor *ip-address vc-id* **encapsulation mpls** [**manual**] [**no-switching-tlv**] [**tnl-policy** *policy-name*]

no neighbor *ip-address* vc-id

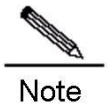
Parameter description

Parameter	Description
ip-address	Specifies the peer IP address.
vc-id	Specifies the PW ID, in the range from 1 to 2147483647.
manual	Specifies a static PW (Default: dynamic PW).
no-switching-tlv	Not supports switching-tlv (Default: supported).
tnl-policy *policy-name*	Specifies the tunnel policy.

Defaults N/A

Command mode Switching-VFI configuration mode

Usage guidelines



Note One switching-VFI instance can be configured with up to two pseudo wires and the pseudo wires can not share one peer.

Examples The following example configures pseudo wires for a switching-VFI instance.

```
Ruijie(config)# l2 vfi ms-pw switching
Ruijie(config-vfi)# neighbor 1.1.1.1 10 encapsulation mpls
Ruijie(config-vfi)# neighbor 1.1.1.2 11 encapsulation mpls
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

neighbor next-hop-unchanged (L2VPN address family)

Use this command to determine not to change the next hop information when a route is sent to the peer (group).

Use the **no** form of this command to cancel the configuration.

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	Specifies the peer address.
peer-group-name	Specifies the peer group name. The name cannot contain more than 32 characters.
next-hop-unchanged	The next hop is not changed when a route is sent to the BGP peer (group).

Defaults The next hop is changed by default when a route is sent to the EBGP peer.

Command Mode BGP l2vpn address family mode

Usage Guide For cross-domain implementation of Kompella L2VPN that adopts Option C (Multihop MP-EBGP), if the MP-EBGP connection is established through the router reflector between autonomous domains, by default, the next hop is changed to itself when a route is sent to the EBGP peer. To implement

cross-domain in Option C mode of Kompella L2VPN, run this command on the router reflector; otherwise cross-domain forwarding fails.

Configuration Examples

```
Ruijie(config)# router bgp 60
Ruijie(config-router)# address-family l2vpn vpls
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 (group).

Platform Description N/A

neighbor send-community

Use this command to enable the BGP extended community attribute. By default, the BGP extended community attribute is enabled when the **neighbor activate** command is used for the first time.

neighbor {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

no neighbor {*ip-address* | *peer-group-name*} [both | standard | extended]

Parameter Description

Parameter	Description
ip-address	IP address
peer-group-name	Specifies the peer group name. The name cannot contain more than 31 characters.
both	(Optional) Sends the standard and extended community attributes.
standard	(Optional) Sends only the standard community attribute.
extended	(Optional) Sends only the extended community attribute.

Defaults No community attribute is sent to a BGP neighbor by default. When exchange of L2vpn address family information is activated for the first time, this attribute is enabled by default.

Command Mode BGP l2vpn address family configuration mode

Usage Guide If a peer group is specified during configuration, all members of the peer group inherit the configuration attribute of this command. By default, this attribute is enabled when the **neighbor activate** command is used for the first time.

Configuration Examples

```
Ruijie# config terminal
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family l2vpn vpls
Ruijie(config-router-af)# neighbor 10.10.10.1 activate
```

```
Ruijie(config-router-af)# neighbor 10.10.10.1 send-community extended
```

Related Commands

Command	Description
address-family l2vpn	Enters l2vpn VPLS or VPWS address family configuration mode.

Platform Description N/A

neighbor tnl-policy(VPLS mode)

Use this command to apply a tunnel policy to the PW used by Kompella VPLS. Use the **no** form of this command to remove the configuration.

neighbor *ip-address* **tnl-policy** *policy-name*

no neighbor *ip-address* **tnl-policy**

Parameter description

Parameter	Description
ip-address	Specifies the VPLS neighbor address.
policy-name	Specifies the tunnel policy name.

Defaults The tunnel selection policy is applied by default.

Command mode VFI configuration mode

Usage guidelines This command is only valid for the L2VPN service of Kompella VPLS.

Examples The following example configures VPLS and applies tunnel policy tnl-pol to neighbor 1.1.1.1.

```
Ruijie(config)# l2 vfi vpls-name vpnid 26 autodiscovery
Ruijie(config-vfi)# neighbor 1.1.1.1 tnl-policy tnl-pol
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

ping mpls pseudowire

Use this command to check the PW connectivity.

ping mpls pseudowire { *ip-address vc-id* [**segment** *segment-number*] | **kompella** *vfi_name local_site_id remote_site_id* **rd** *remote_rd* } { **label-alert** | **ttl-expiry** } [**repeat** *repeat*] [**timeout** *timeout*] [**size** *size*] [**interval** *mseconds*] [**source** *ip-address*] [**destination** *ip-address*] [**pad** *pattern*] [**reply mode** { **ipv4** | **router-alert | control-channel** }] [**verbose**]

Parameter description

Parameter	Description
ip-address	Specifies the PE IPv4 address of a static or Martini PW.
vc-id	Specifies the ID of a static or Martini PW.
segment *segment-number*	(Optional) Specifies the PW segment to be ping.
vfi_name	Specifies the VFI instance name of a Kompella PW.
local_site_id	Specifies the local VE ID of a Kompella PW.
remote_site_id	Specifies the peer VE ID of a Kompella PW.
rd *remote_rd*	Specifies the peer RD value of a Kompella PW.
label-alert | ttl-expiry	Specifies the channel type: **lablel-alert**: Type 2. **ttl-expiry**: Type 3.
repeat *repeat*	(Optional) Specifies the Echo Request retransmission times, in the range from 1 to 2147483647. Default: 5.
timeout *timeout*	(Optional) Specifies the timeout time, in the range from 0 to 3600 seconds. Default: 2.
size *size*	(Optional) Specifies the packet size, in the range from 84 to 18024. Default: 84
interval *mseconds*	(Optional) Speficies the mimimum interval to send Echo Request packets, in the range from 0 to 3600000 seconds. Default: 0.
source *ip-address*	(Optional) Specifies the source PE address. It serves as the destination IP address in the Echo Reply sent by the peer PE. A static PW must be configured with a source IP address and it must be the local PE IPv4 address. A dynamic PW can use the Router ID of the LDP as its source IP address. If a Kompella PW selects control-channel as its reply mode, it must be configured with the local PE IPv4 address as its source IP address.
destination *ip-address*	(Optional) Specifies the destination IP address from 127/8 (Default: 127.0.0.1).

pad *pattern*	(Optional) Padding mode (Default: 0xABCD).
reply mode { ipv4 | router-alert | control-channel }	(Optional) Specifies a reply mode: **IPv4**: Replay by IPv4 UDP packets **router-alert** : Replay by IPv4 UDP packets carrying the Router Alert Option. **control-channe**l : Reply by control-channel
verbose	(Optional) Shows Echo Reply details. No details is shown by default.

Defaults See Parameter Description

Command mode Privileged EXEC mode

Usage guidelines You can enter the exchange input mode by running the **ping mpls** command.

Note A dynamic single-segment PW, a static PW or a Kompella PW only support single-segment PW connectivity check and support **label-alert** and **ttl-expiry** channels. A dynamic multi-segment PW check does not support **label-alert** channel.

Note The source PE address refers to the peer address of the peer PE. Generally, it is the loopback address of the local PE.

Caution Before running this command, run the **no mpls ip ttl propagate vpn** command on the S-PE device. Otherwise, the ping operation may fail.

Examples The following example checks connectivity of a dynamic PW from local end to 10.10.10.3 with PW ID 2.

```
Ruijie# ping mpls pseudowire 10.10.10.3 2 ttl-expiry verbose
% Total number of PW segments is less than segment number; Adjusting the
segment number to 1
Sending 5, 112-byte MPLS Echoes on Pseudowire, peer address 10.10.10.3, VC
ID 2,
    timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
```

```
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Press Ctrl+C to break.
!   size 84, reply addr 20.20.20.2, return code 3
    [Labels: 1025 Exp: 0]
    Rx Interface: 20.20.20.2
    local 10.10.10.1 remote 10.10.10.3 vc id 2
!   size 84, reply addr 20.20.20.2, return code 3
    [Labels: 1025 Exp: 0]
    Rx Interface: 20.20.20.2
    local 10.10.10.1 remote 10.10.10.3 vc id 2
!   size 84, reply addr 20.20.20.2, return code 3
    [Labels: 1025 Exp: 0]
    Rx Interface: 20.20.20.2
    local 10.10.10.1 remote 10.10.10.3 vc id 2
!   size 84, reply addr 20.20.20.2, return code 3
    [Labels: 1025 Exp: 0]
    Rx Interface: 20.20.20.2
    local 10.10.10.1 remote 10.10.10.3 vc id 2
!   size 84, reply addr 20.20.20.2, return code 3
    [Labels: 1025 Exp: 0]
    Rx Interface: 20.20.20.2
    local 10.10.10.1 remote 10.10.10.3 vc id 2

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/30 ms
```

Related commands	**Command**	**Description**
	N/A	N/A
Platform description	N/A	

ppp ipcp address proxy

Use this command to configure the proxy address of the IPCP address option negotiation for the PPP.

ppp ipcp address proxy *ip-address*

no ppp ipcp address proxy

Parameter Description	**Parameter**	**Description**
	ip-address	Proxy address used during IPCP negotiation of PPP

Defaults The proxy address for PPP IPCP negotiation is not configured by default.

Command Mode Interface configuration mode

Usage Guide For the l2vpn of heterogeneous media interworking, the l2vpn of CE terminates on the PE. Therefore, if the CE and PE on one end use PPP for access, the negotiation of the PPP protocol occurs between the PE and CE. As the PE does not know the address of the remote CE, use this command to configure the proxy address on the PE in order to enable the PE to carry the IP address of the remote CE in the IPCP address configuration option to the local CE.

Configuration Examples The following example displays the configuration that enables the PE to provide the heterogeneous media l2vpn service. In this example, the interface used by the PE to connect to the CE encapsulates the PPP protocol.

```
Ruijie# configure terminal
Ruijie(config)# interface pos 1/0
Ruijie(config-if-pos1/0)# encapsulation ppp
Ruijie(config-if-pos1/0)# ppp ipcp address proxy 192.168.1.1
Ruijie(config-if-pos1/0)# xconnect 10.10.10.3 2 encapsulation mpls ip-interworking
Ruijie(config-if-pos1/0)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

rd (Kompella l2vpn)

Use this command to configure the RD value of the Kompella l2vpn vfi instance.

rd *rd_value*

Parameter Description

Parameter	Description
rd_value	RD value

Defaults No RD value is configured by default.

Command Mode VFI configuration mode

Usage Guide This command is valid only for the VPLS and VPWS implemented in Kompella mode. It is invalid for the VPLS implemented in Martini mode.

To configure a Kompella l2vpn instance, configure RD before configuring other parameters.
If the RD value is configured for a Kompella l2vpn instance, the RD value can neither be modified nor deleted. To modify the RD value, delete the Kompella l2vpn instance, create it again, and configure a new RD value for it. An l2vpn vfi instance can have only one RD value.

Configuration Examples

The following example configures the RD value of the Kompella VPLS.

```
Ruijie(config)# l2 vfi vpls-1 vpnid 1 autodiscovery
Ruijie(config-vfi)# rd 100:1
```

The following example configures the RD value of the Kompella VPWS.

```
Ruijie(config)# l2 vfi vpls-2 vpnid 2 point-to-point
Ruijie(config-vfi)# rd 200:1
```

Related Commands

Command	Description
show bgp l2vpn	Displays information of the Kompella l2vpn instance.
site-id	Configures the site ID of the vfi instance.
route-target	Configures the route-target attribute of the vfi instance.
show mpls vfi	Displays information of the l2vpn vfi instance.

Platform Description

N/A

route-target (Kompella l2vpn)

Use this command to configure the route target (RT) attribute of a Kompella l2vpn instance.
Use the **no** form of this command to cancel the configuration.
route-target {**import|export|both**} *rt_value*
no route-target {**import|export|both**} *rt_value*

Parameter Description

Parameter	Description
import	Sets the import RT value.
export	Sets the export RT value.
both	Sets the import and export values.

Defaults

The RT value is not defined by default.

Command Mode

VFI configuration mode

Usage Guide

This command is valid only for the VPLS and VPWS implemented in Kompella mode. It is invalid for the VPLS implemented in Martini mode.
You can configure multiple RT attribute values for a Kompella l2vpn instance and specify **import/export/both**. Each of these RTs can be the mark of the l2vpn vfi instance.
If you specify the **import** and **export** attributes of the RT for an l2vpn vfi instance at the same time, it

is considered that you configure the **both** attribute of the RT.

For different vfi instances of a PE, it is recommended not to configure the same RT. Otherwise, the two vfi instances on the local PE cannot interwork with each other, which means that the RT does not support the interworking between vfi instances on the local PE.

Configuration Examples

The following example configures the RT value of the VPLS instance.

```
Ruijie(config)# l2 vfi vpls1 vpnid 1 autodiscovery
Ruijie(config-vfi)# route-target both 200:1
```

The following example configures the RT value of the VPWS instance.

```
Ruijie(config)# l2 vfi vpws1 vpnid 2 point-to-point
Ruijie(config-vfi)# route-target both 300:1
```

Related Commands

Command	Description
l2 vfi	Creates an l2vfi instance.
rd	Configures the RD value of the vfi instance.
site-id	Configures the site ID of the vfi instance.
show mpls vfi	Displays information of the l2vpn vfi instance.

Platform Description

N/A

show bgp l2vpn

Use this command to display the information about BGP l2vpn.

show bgp l2vpn {**vpls|vpws**} **all** [*ve-id:offset* | **neighbor** *ip-address* |**summary**]

show bgp l2vpn {**vpls|vpws**} **rd** *vpn_rd* [*ve-id:offset*]

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 NLRI information of all VPLS or VPWS instances.
vpn-rd	Displays the VPLS instance information of the specified RD.
vfi-name	VFI instance name
neighbor address	BGP neighbor address
ve_id:offset	Displays the vfi instance information of the specified ve_id:offset.
summary	Displays the main information about bgp l2vpn, including the site ID, offset, label base, and next hop information.

Defaults

N/A

Command Mode Privileged EXEC mode

Usage Guide The **show bgp l2vpn vpls** command can be used to display locally configured VPLS information, including the RD value, site ID, label block offset, and label base. The related VPLS configuration information can be viewed on the BGP only when the configuration of the VPLS instance is complete.

Configuration Examples

```
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         ?
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         ?

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 So0:12345:11 So0:0.0.48.58:11
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
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 1
```

Field	Description
BGP table version	BGP table version
Local Router ID	Local Router ID, usually the loopback address
status codes	Status codes: s – The route is suppressed. d – The route oscillation is shielded. h – History route, unavailable route * – Effective route > – The best route I – IBGP route r – RIB failed the installation of routing table s – Old route
Origin Codes	Origin Codes: i – IGP e – EGP ? - Incomplete
Network	Network routing information in the format of aa:bb. aa represents the site ID, and bb represents the label block offset.
Next hop	IP address of the next hop
Metric	If displayed, it represents the route metric.
LocPrf	Local priority
Path	Autonomous domain path to the destination network
Route Distinguisher	RD of VPLS

Related Commands

Command	Description
address-family l2vpn	Enables the l2vpn VPLS address family.

Platform Description N/A

show bgp l2vpn connections

Use this command to display the connection information of Kompella VPLS or VPWS PW.

show bgp l2vpn {vpls|vpws} all connections [**vfi** *vfi_name*] [**neighbor** *address*] [**site-id** *id*]

[**detail**]

Parameter Description

Parameter	Description
vfi *vfi_name*	Displays the PW information of the specified vfi instance.
neighbor *address*	Displays information about the Kompella vfi PW established with a neighbor.
site-id *id*	Displays the connection information of all VFI instances with the specified local site ID.
detail	Displays the detailed connection information of the specified l2vpn.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the local configuration and remote information of L2 VFI. If there is no remote site information, only local information is displayed.

Configuration Examples Example 1:

```
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           --            --
```

Example 2:

```
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
```

Field	Description
vfi	Name of the vfi instance, with (n) indicating the VPN ID of the vfi

	instance
Local Site	Local site ID
Connect-Site	Connected remote site ID
Status	PW status (Up or Down)
Neighbor	Neighbor address of the created PW
Remote-Label	Remote label of the created PW, that is, the outgoing label
Local-Label	Local label of the created PW, that is, the incoming label

Example 1:

```
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
```

Example 2:

```
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: --
```

Field	**Description**
vfi	Name of the l2vpn vfi instance, with (n) indicating the VPN ID and l2vpn vfi type (VPWS or VPLS) of the l2vpn vfi instance
Local site	Local site ID
Label-base	Label block base
Offset	Label block offset
Range	Maximum number of sites for access

Remote site	Remote site ID. One local site may be mapped to multiple remote sites. Connected: A connection is set up with the remote site. Unconnected: No connection is set up with the remote site.

Related Commands

Command	Description
xconnect	Binds the interface to VPWS PW, and creates the VPWS PW instance; or binds the interface to the Martini or Kompella VPLS instance.
l2 vfi	Configures the VPLS instance.

Platform Description N/A

show ip ref mpls forwarding-table vfi

Use this command to display the MAC forwarding information of the VPLS instance quick forwarding plane.

show ip ref mpls forwarding-table vfi [*vfi_name*] **{mac-address-table** *[H.H.H]***|statistics}**

Parameter Description

Parameter	Description
vfi *vfi_name*	Specifies the VPLS instance whose information is to be displayed. If this parameter is not specified, information of all VPLS instances will be displayed.
mac-address-table	Displays the MAC forwarding table information.
H.H.H	Displays the specific MAC address forwarding information.
statistics	Displays the forwarding statistics of the VPLS instance.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display forwarding entries and forwarding statistics of the VPLS instance. This command is invalid for the Kompella VPWS.


Note

The quick forwarding function of the interface must be enabled for routers.
Switches do not support the forwarding statistics function.

Configuration

```
Ruijie# show ip ref  forwarding-table vfi aa mac-address-table
```

Examples

```
VPLS: aa(10)
  aging time : 300 sec , mtu : 1500
  total number of addresses : 4
  maximum number of addresses : 256
  mac-limit action : discard
  mac-limit alarm : enable
  MAC Address     VC Label  Peer Address  Type       Interface
  001a.a915.3218   1024     2.2.2.2         D            --
  0022.1132.3425    --       --              S          Gi1/1
  0022.1135.0a91  1025       3.3.3.3         D            --
  0022.2002.3126   --        --              D          Gi1/1
```

Field	Description
MAC Address	MAC address information
VC Label	VC label. If the outgoing interface of the MAC address is VC, this field indicates the VC label that needs to be pressed in. If the outgoing interface of the MAC address is the AC end, this field is invalid.
Peer Address	VPLS neighbor information. If the outgoing interface of the MAC address is VC, this field indicates the address of the VC peer. If the outgoing interface of the MAC address is the AC end, this field is invalid.
Type	Indicates the MAC address type. D indicates that the MAC address is dynamically learnt. S indicates that the MAC address is statically configured.
Interface	If the outgoing interface of the MAC address is VC, this field is invalid. If the outgoing interface of the MAC address is the AC end, this field indicates the information of the outgoing interface.

```
Ruijie# show ip ref mpls forwarding-table vfi aa statistics
VPLS: aa(10)
  packet discard: 200
  packet reserve: 200
  packet forward:200
```

Field	Description
discard	Number of discarded packets
reserve	Number of packets for sending progress policies
forward	Number of forwarded packets

Related Commands

Command	Description
show mpls forwarding-table	Displays the VPLS forwarding table of the progress forwarding plane.

Platform Description N/A

show mpls forwarding-table vfi

Use this command to display the MAC forwarding information forwarded by MPLS of the VPLS instance.

show mpls forwarding-table vfi [*vfi_name*] **{mac-address-table** *[H.H.H]***|statistics}**

Parameter Description

Parameter	Description
vfi *vfi_name*	Specifies the VPLS instance whose information is to be displayed. If this parameter is not specified, information of all VPLS instances will be displayed.
mac-address-table	Displays the MAC forwarding table information.
H.H.H	Displays the specific MAC address forwarding information.
statistics	Displays the forwarding statistics of the VPLS instance.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display forwarding entries and forwarding statistics of the VPLS instance. This command is invalid for the Kompella VPWS.

The quick forwarding function of the interface must be enabled for routers.

Switches do not support the forwarding statistics function.

Configuration Examples

```
Ruijie# show mpls forwarding-table vfi aa mac-address-table
VPLS: aa(10)
  aging time : 300 sec , mtu : 1500
  total number of addresses : 4
  maximum number of addresses : 256
  mac-limit action : discard
  mac-limit alarm : enable
  MAC Address     VC Label  Peer Address  Type       Interface
  001a.a915.3218   1024    2.2.2.2          D            --
  0022.1132.3425    --      --               S           Gi1/1
  0022.1135.0a91  1025      3.3.3.3           D            --
  0022.2002.3126   --       --                 D          Gi1/1
```

Field	Description
MAC Address	MAC address information
VC Label	VC label. If the outgoing interface of the MAC address is VC, this

	field indicates the VC label that needs to be pressed in. If the outgoing interface of the MAC address is the AC end, this field is invalid.
Peer Address	VPLS neighbor information. If the outgoing interface of the MAC address is VC, this field indicates the address of the VC peer. If the outgoing interface of the MAC address is the AC end, this field is invalid.
Type	Indicates the MAC address type. D indicates that the MAC address is dynamically learnt. S indicates that the MAC address is statically configured.

Related Commands

Command	Description
show ip ref mpls forwarding-table vfi	Displays the VPLS forwarding table of the quick forwarding plane.

Platform Description N/A

show mpls l2transport switching vfi

Use this command to show the switching VFI information. Use the **no** form of this command to remove the configuration.

show mpls l2transport switching vfi [*name***]**

Parameter description

Parameter	Description
name	Specifies the switching VFI information.

Defaults N/A

Command mode Privileged EXEC mode

Usage guidelines If no switching VFI instance is specified, all switching VFI will be shown.

Examples The following example shows the switching VFI information.

```
Ruijie#show mpls l2transport switching vfi
Total switching vfi count: 1
VFI name: ms-pw
 Control word: no, VC Type: ethernet, GroupID 0
 MTU: 1500, Interface Desc: n/a
 PW Switching Point:
```

```
Peer-Address   VC-ID   Local circuit  Description
1.1.1.1         10      1.1.1.2:11   attatach-BJ-SH

Control word: no, VC Type: ethernet, GroupID 0
 MTU: 1500, Interface Desc: n/a
 PW Switching Point:
Peer-Address   VC-ID   Local circuit  Description
1.1.1.2         11      1.1.1.1:10   attatach-BJ-SH
```

Related commands	Command	Description
	N/A	N/A
Platform description	N/A	

show mpls l2transport vc

Use this command to display the information of VPWS PW and VPLS PW.

show mpls l2transport vc [[*vc_id* [*ip-address*]] | [**interface** *interface_name*]] [**detail**] [**count**]

Parameter Description

Parameter	Description
vc_id	ID of the PW to be displayed
ip_address	LSR ID of the peer of the PW to be displayed
interface *interface_name*	Interface on which the bound VPWS PW is to be displayed. This parameter is invalid for the VPLS PW.
count	Displays the statistics of the PW.
detail	Displays detailed information of the PW.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide For Martini VC, an ID can be used by multiple PWs. Therefore, the **show mpls l2transport vc** *vc-id* command may display the information of multiple PWs. You can use the **peer** parameter to filter these PWs.

Configuration Examples Example 1:

```
Ruijie# show mpls l2transport vc 1 detail
VC ID: 1 (manual), Status: up
Signaling protocol: LDP
Local interface : vlan 10(up)
Peer address: 192.168.0.1
```

```
VC type: ethernetvlan(vpws)  VC mode:tagged
Local/Remote VC label: 100/200
Local/Remote group id: 0/0
Local/Remote mtu: 1500/1500
Control word : disable
 Depend LSP info:
Output interface: Gi 3/3, imposed label stack { 200 ,501 }
Create time: 01:01:30 Last change time: 00:01:30  Up time: 00:01:30
```

Example 2:

```
Ruijie# show mpls l2transport vc detail
VC ID: 2147483650 (auto), Status: up
Signaling protocol: BGP
Local/Remote site id: 8/9
Peer address: 192.168.0.1
VC type: vlan(vpls-hub) VC mode:tagged
Attached VFI: vpls1
Local/Remote VC label: 16384/8097
Local/Remote group id: --/--
Local/Remote mtu: 1500/1500
Control word : disable
 Depend LSP info:
Output interface: Gi 3/3, imposed label stack { 8097 ,501 }
Create time: 01:01:30 Last change time: 00:01:30  Up time: 00:01:30

VC ID: 100 (manual), Status: up
Signaling protocol: LDP
Local interface : vlan 10 (up)
Peer address: 192.168.0.1
VC type: ethernet(vpws)  VC mode:raw
Local/Remote VC label: 100/200
Local/Remote group id: 0/0
Local/Remote mtu: 1500/1500
Control word : disable
 Depend LSP info:
Output interface: Gi 3/3, imposed label stack { 200 ,501 }
Create time: 01:01:30 Last change time: 00:01:30  Up time: 00:01:30

Ruijie# show mpls l2transport vc count
 VPLS VC count: 20
 VPWS VC count: 15
 Up VC count: 30 (VPLS: 15, VPWS 15)
 Down VC count: 5 (VPLS: 0, VPWS 5)
 Total VC count: 35
```

Field	Description

VC ID	Unique ID of the VC. **manual**: The VC ID is manually configured. **auto**: The VC ID is automatically generated. The IDs of VCs corresponding to kompella VPWS and VPLS are automatically generated. Status indicates the status (up or down) of the VC.
Signaling Protocol	Signaling protocol (BGP or LDP)
Local/Remote site id	For Kompella VPLS or Kompella VPWS, this field indicates the local and remote site IDs used to establish the VC. For Martini VPLS or Martini VPWS, this field is not displayed.
Local interface	Interface that the VC is bound with. This field is valid only for VCs of VPWS. It is invalid for VCs of VPLS. Up/down indicates the status of the interface.
Peer address	Peer IP address of the VC
VC type	Type of the VC. For VPLS, only ethernet and vlan are available. For VPWS, PPP and HDLC are also available. **vpws**: The VC is a VC of the VPWS service. **vpls-hub**: The VC is a hub VC of the VPLS. **vpls-spoke**: The VC is a spoke VC of the VPLS.
Attached VFI	For Kompella VPLS or VPWS, this field indicates the VFI to which the VC belongs. For Martini VPLS or VPWS, this field is not displayed.
VC mode	VC mode: tagged or raw. For non-Ethernet VCs, this field is not displayed.
Local ce mac	If the VC type is heterogeneous media, and the local end is an Ethernet, this field indicates the locally configured CE MAC.
Local/Remote VC label	Private network labels assigned to the VC by the local and peer ends. If no label has been assigned, this field is displayed as --.
Request ingress PE rewrite vlan	Determines whether to request the incoming interface to rewrite vlan. The values enable and disable are available.
Local/Remote group id	IDs of the groups to which the VC belongs on the local and peer ends. If the VC is not UP, this field is displayed as --. This field is valid only for PWs established in LDP mode. This field is invalid and not displayed for PWs established by BGP signaling.
Local/Remote mtu	The MTU value of the VC negotiated by the local and peer ends. If the VC is not UP, this field is displayed as --.
Control word	Determines whether control word is enabled. The values enable and disable are available.
Depend LSP info	Output interface: Outgoing interface used to transmit the VC traffic on the public network imposed label stack: Label stack { 200, 501 } carried by the VC data. 200 is the VC label, and 501 is the dependent LSP label.
Create time	Time used to create the VC
Last change time	Time used for the last VC status change
Up time	Time for which the VC is in the UP state

Related Commands

Command	Description
xconnect	Binds the interface with the VPWS PW and creates the VPWS PW instance; or binds the interface with the Martini or Kompella VPLS instance.
neighbor	Configures the VPLS neighbor.

Platform Description N/A

show mpls l2vc ftn-table

Use this command to display the FTN table information of PW.

show mpls l2vc ftn-table

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# show mpls l2vc ftn-table
Local intf Dest address  VC ID  VC_label   Out intf
---------- ------------- ------ --------  --------
-            2.2.2.2         1      1024       GigabitEthernet 1/1
-            3.3.3.3         1      21         GigabitEthernet 1/2
```

Related Commands

Command	Description
xconnect	Binds the interface with the VPWS PW and creates the VPWS PW instance; or binds the interface with the VPLS instance.
neighbor	Configures the VPLS neighbor.

Platform Description N/A

show mpls ldp vc

Use this command to display the PW information of the LDP.

show mpls ldp vc {**all** | **vpws** | **hub | spoke**} [*vc-id*]

Parameter Description

Parameter	Description
all	Displays all types of PWs.
vpws	Displays VPWS-type PWs (including unknown-type PWs).
hub	Displays hub-type VPLS PWs.
spoke	Displays spoke-type VPLS PWs.
vc-id	Displays information of the specified PW.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
Ruijie# show mpls ldp vc all
Total VC Count: 1
VC: vcid: 1, peer: 3.3.3.3
  local info:
    vpn_id: 1, vc bind type: vpls hub vc (vpls-name vpls1)
    Local vc type: Ethernet VLAN, local group id: 0, local mtu: 1500
    local prefer use Control Word: no, local use Control Word: no
  Remote info:
    remote vc type: Ethernet VLAN, remote group id: 0, remote mtu: 1500
    remote use Control Word: no
    remote label: 21
  VC info:
    state: (0x27) create | map_send | map_recv | AC up
    session: 3.3.3.3:0
    local_label: 1027
    last send message id: 398
    last recv message id: 105
create time: 02:47:06, last change time: 01:17:29, up time: 01:17:29
```

Field	Description
Total VC Count	Number of VCs in the LDP
Vcid	Unique VC ID
Peer	IP address of the VC peer
local info	Local VC configuration
vpn id	ID of the VPN that the VC belongs to, VC ID for VPWS VC and

	VPLS ID for VPLS VC
vc bind type	Indicates the type of the VC, which may be VPWS VC, VPLS HUB VC, or VPLS SPOKE VC.
local vc type	Local VC type
local group id	Local group ID of VC
local mtu	local MTU of VC
local prefer use Control Word	Indicates whether control word is enabled on the local end.
local use Control Word	Indicates whether the negotiated control word is used.
Remote info	Configuration information of the VC peer
remote vc type	VC type on the peer
remote group id	Peer group ID of the VC
remote mtu	Remote VC MTU
remote use Control Word	Indicates whether control word is enabled on the peer end.
remote label	Label that the peer assigns to the VC
VC info	Other VC information
State	VC status, which can be the combination of any of the following states: None: No state Create: Create map_send: The label mapping message is sent. map_recv: The label mapping message is received. withdraw_send: The label mapping message is withdrew. req_send: The label request message is sent AC up: AC bound by the VC is up. AC down: AC bound by the VC is down.
Session	LDP session exchanging VC information
local label	Label locally assigned to the VC
last send message id	ID of the last sent LDP message carrying the VC message
last recv message id	ID of the last received LDP message carrying the VC message
create time	Time used to create the VC on the LDP
last change time	Time used for the last VC change on the LDP
up time	Time for which the VC on the LDP is in the up state

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mpls switching vfi

Use this command to show the switching VFI information. Use the **no** form of this command to remove the configuration.

show mpls switching vfi [**name**]

Parameter description

Parameter	Description
name	Specifies the switching VFI information.

Defaults N/A

Command mode Privileged EXEC mode

Usage guidelines If no switching VFI instance is specified, all switching VFI will be shown.

Examples The following example shows the switching VFI information.

```
Ruijie#show mpls switching vfi
Total switching vfi count: 1
VFI name: ms-pw, Admin State: up
 Description: attatach-BJ-SH
 VFI Type: Switching, MTU: 1500
 PW Encapsulation type: ethernet
 Segment 1:
  Peer-Address   VC-ID    State   Local-label  Remote-label  Signal
  1.1.1.1         10      up       1500        1600        LDP
Segment 2:
  Peer-Address   VC-ID    State   Local-label  Remote-label  Signal
  1.1.1.2         11      up       1510        1610         LDP
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

show mpls ldp vfi

Use this command to display the PW information of the LDP.

show mpls ldp vfi [*name*]

Parameter Description

Parameter	Description
name	Name of the VPLS instance

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Different from the **show mpls vfi** command, this command displays only effective VPLS instances in the LDP.

Configuration Examples

```
Ruijie (config)#show mpls ldp vfi
Total VPLS Count: 1

VPLS: name:vpls1, vpls id: 1, admin state up
Create time: 02:46:28, last change time: 02:46:28
Hub-vc number:2   Spoke-vc number 0
Hub vc info:
VC: vcid: 1, peer: 2.2.2.2
local info:
vpn_id: 1, vc bind type: vpls hub vc (vpls-name vpls1)
Local vc type: Ethernet, local group id: 0, local mtu: 1500
local prefer use Control Word: no, local use Control Word: no
Remote info:
remote vc type: Ethernet, remote group id: 0, remote mtu: 1500
remote use Control Word: no
 remote label: 1024
VC info:
state: (0x27) create | map_send | map_recv | AC up
session: 2.2.2.2:0
local_label: 1026
last send message id: 556
last recv message id: 394
create time: 02:46:28, last change time: 01:00:36, up time: 01:00:36
VC: vcid: 1, peer: 3.3.3.3
local info:
vpn_id: 1, vc bind type: vpls hub vc (vpls-name vpls1)
Local vc type: Ethernet VLAN, local group id: 0, local mtu: 1500
local prefer use Control Word: no, local use Control Word: no
Remote info:
remote vc type: Ethernet VLAN, remote group id: 0, remote mtu: 1500
remote use Control Word: no
remote label: 21
VC info:
state: (0x27) create | map_send | map_recv | AC up
session: 3.3.3.3:0
local_label: 1027
last send message id: 398
last recv message id: 105
```

```
create time: 02:47:06, last change time: 01:17:29, up time: 01:17:29
```

Field	Description
Total VPLS Count	Number of VPLS instances in the LDP
Name	Name of the VPLS instance
vpls id	ID of the VPLS instance
admin state	Administration state of the VPLS instance
Create time	Time used to create the VPLS instance on the LDP
last change time	Time used for the last change of the VPLS instance on the LDP
Hub-vc number	Number of the hub VCs of the VPLS instance
Spoke-vc number	Number of the spoke VCs of the VPLS instance
Hub vc info	Detailed information of all hub VCs of the VPLS instance. For detailed description, see the **show mpls ldp vc** command.
Spoke vc info	Detailed information of all spoke VCs of the VPLS instance. For detailed description, see the **show mpls ldp vc** command.

Related Commands

Command	Description
l2 vfi	Creates a VPLS instance or enters VPLS configuration mode. The **no** form of this command deletes the VPLS instance.
Neighbor	Configures the VPLS neighbor.
xconnect	Binds the interface with the VPWS PW and creates the VPWS PW instance; or binds the interface with the VPLS instance.

Platform Description N/A

show mpls vfi

Use this command to display all configured VFI information or the specified VFI information.

show mpls vfi [*name*]

Parameter Description

Parameter	Description
name	Name of the l2vpn vfi instance

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the optional parameter **name** is not specified, this command displays all VPLS instances and Kompella VPWS instances by default.

Configuration Examples

```
Ruijie#show mpls vfi
Total VFI count: 2
 Autodiscovery VFI count: 1
 Manually VFI count: 1
 Point-to-Point VFI count: 0
 Total VPLS PW count: 4
 Total PW count:4
VFI name:vpls1 (vpnid 1) Admin State:up
  Description: Martini vpls example
  VFI Type: Martini VPLS, Signal: LDP , mtu: 1500
  Maximum num of MAC: 1024
  Mac-limit action: forward
  Mac-limit alarm: enable
  Local Attachment Circuit (AC):
AC Name       AC State
Gi 0/0          Up
  Pw count:2
  Neighbor connected via pseudowires:
  Peer-Address VC-ID Type  State Local-label Remote-label
  2.2.2.2        1      Hub    up     1026          1024
  3.3.3.3        2      Spoke up     1027          21

VFI name:vpls2 (vpnid 2)  Admin State:up
VFI Type: KOMPELLA VPLS, Signal: BGP, mtu: 1500
PW Encapsulation type: ethernet
  Maximum num of MAC: 1024
  Mac-limit action: forward
  Mac-limit alarm: enable
Local Attachment Circuit (AC):
AC Name       AC State
Gi 0/1        Up
Gi 0/2        Down
Matched l2 extcommunity
  Route-Distinguisher: 23:23
Import Route Target: 1:200
Export Route Target: 1:200
Local site-id info:
 Site-id: 1, Site-range: 16
  Pw count:2
  Neighbor connected via pseudowires:
  LSID RSID Peer-Address VC-ID   Type State Local-label Remote-label
  1     2     4.4.4.4  2147483648 Hub   up     8096          1024
1     3     5.5.5.5  2147483649 Hub   up     8097          1024
```

Field	Description
Total VFI count	Total number of configured static VFIs
Autodiscovery VFI count	Number of VFIs using BGP signaling, including the VFI instances of VPWS and VPLS
Manually VFI count	Number of VFIs using LDP signaling, namely the number of VFI instances of Martini VPLS
Point-to-Point VFI count	Number of VPWS VFI instances using BGP signaling
Total VPLS PW count	Number of VPLS PWs
Total PW count	Number of all PWs, including VPWS PWs and VPLS PWs
vfi name(n)	Name of the VPLS instance, with n indicating the VPN ID of the VPLS instance
State	VPLS instance state (up or down)
Signal	Signal
Site id	Site ID
mtu	MTU of the VPLS instance
Route-Distinguisher	RD value, for example, 100:1 or 202.118.239.165:1
Route Target	RT value, for example, 100:1 or 202.118.239.165:1
Local Attachment Circuit	AC bound with the VPLS instance
Pw count	Number of VCs in the VPLS instance
LSID	Local site ID of the VC associated with the VPLS instance
RSID	Remote site ID of the VC peer associated with the VPLS instance
Peer-Address	IP address of the VC peer associated with the VPLS instance
VC-ID	ID of the VC associated with the VPLS instance
Type	Hub: Indicates VPLS hub VC. Spoke: Indicates VPLS spoke VC. P2P: Indicates VPWS VC.
State	State (up or down) of the VC associated with the VPLS instance
local-label	Label assigned to the VC associated with the VPLS instance
remote-label	Received label of the VC associated with the VPLS instance

Related Commands

Command	Description
l2 vfi	Creates a vfi instance or enter VFI configuration mode. The **no** form of this command deletes the vfi instance.

Platform Description N/A

signal

Use this command to specify the PW signaling of l2vpn vfi.

Use the **no** form of this command to restore to the default configuration.

signal bgp

no signal

Parameter Description

Parameter	Description
bgp	Specifies the use of the BGP signaling.

Defaults The PW signaling needs to be configured only in the automatic discovery mechanism, and the BGP signaling is used by default.

Command Mode VFI configuration mode

Usage Guide This command is valid only for the VPLS and VPWS implemented in Kompella mode. It is invalid for the VPLS implemented in Martini mode.
BGP is used as the signaling protocol by default when automatic discovery is enabled.

Configuration Examples

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vpls-name vpnid 10 autodiscovery
Ruijie(config-vfi)#signal bgp
```

Related Commands

Command	Description
encapsulation	Configures the encapsulation mode of Kompella l2vpn.

Platform Description N/A

site-id

Use this command to configure the site information of the PE in the Kompella l2vpn vfi instance and enter site configuration mode. Use the **exit-site-mode** command to exit site configuration mode.
Use the **no** form of this command to delete the configuration of the specified site ID.
site-id *id* **[site-range** *range***]**
no site-id *id*

Parameter Description

Parameter	Description
id	Site ID of the vfi instance, ranging from 1 to 256
range	Number of sites to be accessed, ranging from 1 to 256

Defaults The default range is 16.

Command Mode VFI configuration mode

Usage Guide This command is valid only for the VPLS and VPWS implemented in Kompella mode.

The **site-range** parameter of this command can be used to adjust the number of sites to be accessed by the l2vpn vfi instance, that is, the number of connections between the l2vpn vfi instance of the PE and remote PEs that belong to the same l2vpn site. You can modify the maximum number of remote PEs that can be connected to the instance. If the number is changed to a larger value, it does not affect the l2vpn service. However, if the number is changed to a smaller value, it may interrupt the current l2vpn service and establish a new PW, and forwarding is restored only when the PW is established.

For Kompella l2vpn, use this command to enter vfi-site configuration mode and configure the local interfaces bound with the VPWS or VPLS.

Caution

Different vfi instances on the same PE can be configured with the same ID.

The local ID value is greater than or equal to the remote offset value, and less than the sum of remote size and offset values (that is, the site-range configured on the peer PE).

It is recommended that the maximum number of accessed sites allowed by the same VPLS instance should be the same. Otherwise, the preceding restrictions must be met.

An l2vpn vpls instance can be configured with only one site, and the configured site ID cannot be changed. To change the site ID, delete the site ID and then configure another one.

An l2vpn vpws instance can be configured with several site IDs, and each site ID represents a VPWS site of the instance. Specify the locally bound interface and the remote site to be connected in vfi-site configuration mode. If the specified remote site ID is also configured locally, a sham line cannot be established successfully.

For the Kompella VPWS instance, the site range configuration is not valid in label saving mode.

Configuration Examples The following example configures the site ID of the VPLS instance.

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vpls-name vpnid 25 autodiscovery
Ruijie(config-vfi)# site-id 1
Ruijie(config-vfi-site)# xconnect interface gi 0/1
```

The following example configures the site ID of the VPWS instance.

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vpls-name vpnid 25 point-to-point
Ruijie(config-vfi)# site-id 1
Ruijie(config-vfi-site)# xconnect interface gi 0/2 remote-ce-id 2
```

Related Commands

Command	Description
l2 vfi	Creates an l2vpn vfi instance or enter vfi configuration mode.
rd	Configures the RD information of the vfi instance.
route-target	Configures the RT information of the vfi instance.
show mpls vfi	Displays information of the l2vpn vfi instance.

Platform Description N/A

traceroute mpls pseudowire

Use this command to check the PW connectivity.

traceroute mpls pseudowire { ip-address vc-id { segment segment-number } | kompella vfi_name local_site_id remote_site_id rd remote_rd } { label-alert | ttl-expiry } [timeout timeout] [source ip-address] [destination ip-address] [reply mode { ipv4 | router-alert | control-channel }] [verbose]

Parameter description

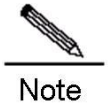
Parameter	Description
ipv4-address	Specifies the PE IPv4 address of a static or Martini PW.
vc-id	Specifies the ID of a static or Martini PW.
segment *segment-number*	(Optional) Specifies the PW segment to be ping.
vfi_name	Specifies the VFI instance name of a Kompella PW.
local_site_id	Specifies the local VE ID of a Kompella PW.
remote_site_id	Specifies the peer VE ID of a Kompella PW.
rd *remote_rd*	Specifies the peer RD value of a Kompella PW.
label-alert | ttl-expiry	Specifies the channel type: **lablel-alert**: Type 2. **ttl-expiry**: Type 3.
timeout *timeout*	(Optional) Specifies the timeout time, in the range from 0 to 3600 seconds. Default: 2.
source *ip-address*	(Optional) Specifies the source PE address. It serves as the destination IP address in the Echo Reply sent by the peer PE. A static PW must be configured with a source IP address and it must be the local PE IPv4 address. A dynamic PW can use the Router ID of the LDP as its source IP address. If a Kompella PW selects control-channel as its reply mode, it must be configured with the local PE IPv4 address as its source IP address.
destination *ip-address*	(Optional) Specifies the destination IP address from 127/8 (Default: 127.0.0.1).

reply mode { ipv4 | router-alert | control-channel }	(Optional) Specifies a reply mode: **IPv4**: Replay by IPv4 UDP packets **router-alert** : Replay by IPv4 UDP packets carrying the Router Alert Option. **control-channe**l : Reply by control-channel
verbose	(Optional) Shows Echo Reply details. No details is shown by default.

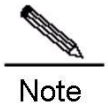
Defaults See Parameter Description

Command mode Privileged EXEC mode

Usage guidelines You can enter the exchange input mode by running the **traceroute mpls** command.


Note

A dynamic single-segment PW, a static PW or a Kompella PW only support single-segment PW connectivity check and support **label-alert** and **ttl-expiry** channels. A dynamic multi-segment PW check does not support **label-alert** channel.


Note

The source PE address refers to the peer address of the peer PE. Generally, it is the loopback address of the local PE.


Caution

Before running this command, run the **no mpls ip ttl propagate vpn** command on the S-PE device. Otherwise, the ping operation may fail.

Examples The following example checks connectivity of a dynamic PW from local end to 10.10.10.3 with PW ID 2.

```
Ruijie#traceroute mpls pseudowire 10.10.10.3 2 segment 1 ttl-expiry
Tracing PW segments within range [1-1], peer address 10.10.10.3, VC ID 2,
timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
```

```
Press Ctrl+C to break.
  0 20.20.20.1     MRU 1500 [Labels: 1025 Exp: 0]
! 1 20.20.20.2     60 ms [Labels: 1025 Exp: 0]
                local 10.10.10.1 remote 10.10.10.3 vc id 2
```

Related commands	Command	Description
	N/A	N/A
Platform description	N/A	

unknown-frame unicast

Use this command to enable forwarding control on VPLS unknown unicast packets. Use the **no** form of this command to remove the configuration.

unknown-frame unicast [**ac-ac | ac-pw | pw-ac**] **discard**

no unknown-frame unicast [**ac-ac | ac-pw | pw-ac**] **discard**

Parameter description

Parameter	Description
ac-ac	Not broadcasts unknown unicast packets from an AC or a Spoke PW to the AC or the Spoke PW.
ac-pw	Not broadcasts unknown unicast packets from an AC or a Spoke PW to the Hub PW.
pw-ac	Not broadcasts unknown unicast packets from a Hub PW to the AC or the Spoke PW.

Defaults Unknown unicast packets are broadcast by default.

Command mode VFI configuration mode

Usage guidelines If this command is not configured, unknown unicast packets from an AC or a Spoke PW will be broadcast to the Hub PW, the AC and the Spoke PW; unknown unicast packets from a Hub PW will be broadcast to the AC and the Spoke PW. In some cases, the local PE, working as the UPE, does not learn the MAC address of the NPE. When it receives the unknown unicast packets from an AC or a Spoke PW to the NPE, it broadcasts the packets only to the NPE.

Examples The following example enables forwarding control on VPLS unknown unicast packets

```
Ruijie# config terminal
Ruijie(config)# l2 vfi vfi_a vpnid 1
```

Ruijie(config-vfi)# unknown-frame unicast ac-ac discard

Related commands	Command	Description
	N/A	N/A
Platform description	N/A	

vc-withdraw-expect-release

Use this command to enable the LDP to wait the release of PW label from the peer after the LDP sends the PW label withdraw message.
Use the **no** form of this command to restore to the default configuration.
vc-withdraw-expect-release
no vc-withdraw-expect-release

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The LDP waits the release of PW label from the peer by default after sending the PW label withdraw message.

Command Mode config-mpls-router configuration mode

Usage Guide After this command is executed, the LDP releases the label only after receiving the PW label release message from the peer. For example, the LDP sends the PW label release message for AC down. If the LDP does not receive the PW label release message from the peer, the LDP will not resend the PW label mapping message when AC is up and then the PW is up again, until it receives the PW label release message from the peer or the **no vc-withdraw-expect-release** command is executed.

Configuration Examples

```
Ruijie(config-mpls-router)#vc-withdraw-expect-release
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

xconnect

Use this command to enable VPWS service on the interface.

xconnect *vc_peer vc_id* **encapsulation mpls** [**ethernet** | **ethernetvlan|ppp|hdlc|[ip-interworking**[**local-ce mac** *mac*]]] [**raw** |**tagged**] [**send-vlanrewrite-req** | **not-send-vlanrewrite-req**] [*group-id*] [*mtu*]

Use the **no** form of this command to cancel the Martini VPWS service on the interface.

no xconnect

Parameter Description

Parameter	Description
vc_id	ID of the PW service instance, in the range from 1 to 2147483647
vc_peer	LSR ID of the peer in the form of A.B.C.D
ethernet	Specifies the PW type as ethernet.
ethernetvlan	Specifies the PW type as vlan.
ppp	Specifies the PW type as ppp encapsulation.
hdlc	Specifies the PW type as hdlc encapsulation.
ip-interworking	Specifies the PW encapsulation type as ip-interworking, indicating that the CE link types on the two ends of L2 VPN are inconsistent and the heterogeneous media interworking feature of L2 VPN must be used. When ip-interworking is used, user layer-3 data (that is, IP packets) instead of layer-2 packets are transparently transmitted on the MPLS network. For heterogeneous media L2 VPN, on receiving a packet from the CE, the PE decapsulates the link layer, encapsulates the MPLS label into the IP packet, and sends the IP packet to the peer PE through the MPLS network. The peer PE encapsulates the received IP packet according to its link layer protocol and sends the packet to the CE that it connects to. Link layer control packets sent by the CE are processed by the PE and will not be transmitted on the MPLS network. All non-IP packets are discarded and will not be transmitted on the MPLS network.
local-ce mac *mac*	If the PW type is heterogeneous media interworking, and the PE and CE connects to Ethernet lines, the MAC address of the CE must be configured on the PE. If the MAC address is not configured, the destination MAC uses the broadcast address for encapsulation by default.
raw	Specifies the encapsulation mode as raw. It is valid only when the PW type is ethernet or ethernetvlan.
tagged	Specifies the encapsulation mode as tagged. It is valid only when the PW type is ethernet or ethernetvlan.
send-vlanrewrite-req	Sends the VLAN rewrite request message to the peer. It is valid only when the PW type is ethernetvlan.
not-send-vlanrewrite-req	Do not send the VLAN rewrite request message to the peer. It is valid only when the PW type is ethernetvlan.
group-id	Group ID of the specified PW, in the range from 0 to 4294967295, with the default value of 0
mtu	mtu value of the specified PW, in the range from 46 to 9216

Defaults No Martini VPWS service is enabled on the interface by default.
For Martini VPWS, the ethernet-type PW and raw encapsulation mode are used by default.

Command Mode Interface configuration mode

Usage Guide The **mtu** parameter in this command indicates the size of a packet that can be transmitted by the PW, that is, the length of the user layer-2 packet and PW encapsulation. By default, if the PW does not enable control word, and two labels are encapsulated, the length of the user Ethernet packet that can be transmitted is 1492 bytes, of which 8 bytes are the PW encapsulation (two labels). If the mtu negotiated by the PW signaling protocol is modified, the mtu (usually the value of PW mtu minus the PW encapsulation) of the user service access interface must be adjusted. In addition, the mtu of the outgoing interface on the PW's public network side must be modified to be the same as the PW mtu for proper forwarding. You can run the **mtu** command to modify the mtu of the interface.
If Martini mode is used to establish a PW, the mtus and PW types configured on the two ends of the PW must be consistent. Otherwise, the PW cannot be UP.
For heterogeneous media L2 VPN interworking, if the PE and CE use Ethernet interfaces or Ethernet subinterfaces for connections, it is not allowed to connect to multiple CEs through the Hub or layer-2 switch. Otherwise, forwarding may fail due to incorrect destination MAC of the CE.
After an interface is bound with VPWS, the PW type, encapsulation mode, and mtu cannot be modified. If a modification is required, delete the VPWS service bound with the interface and then set the parameters again.
For switches, if the L2VPN service is accessed through the Trunk interface, it is not allowed to bind VPLS and VPWS on the default VLAN (VLAN 1).
The switch is bound to the SVI member interfaces of VPLS and VPWS, and the member interface type is trunk or hybrid. IPv4 or IPv6 multicast routing, igmp snooping, and mld snooping cannot be enabled on all the SVIs of these member interfaces.

Configuration Examples The following example binds interface gi2/1 to VPWS.

```
Ruijie(config)#int gi 2/1
Ruijie(config-if)# xconnect 1.1.1.1 1 encapsulation mpls
```

Related Commands

Command	Description
show mpls l2transport vc	Displays information of the PW service instance.

Platform Description N/A

xconnect interface

Use this command to enable the Kompella l2vpn service and connect the local interface to the remote CE of the vfi.
xconnect interface *interface-type interface-number* [**remote-ce-id** *id*]
Use the **no** form of this command to cancel the l2vpn service.

no xconnect

Parameter Description

Parameter	Description
interface-type interface-number	Configures the interface type and interface ID
id	Remote CE ID of the vfi. It is valid only for the Kompella VPWS. It is not required for Kompella VPLS.

‘

Defaults The interface does not provide the l2vpn service by default.
For Kompella l2vpn, the ethernet-type PW and raw encapsulation mode are used by default.

Command Mode VFI site configuration mode

Usage Guide It is recommended to run the **encapsulation mpls** command to set the VPWS PW type as **ethernetvlan** when the local subinterface is used to access the VPWS service, and set the VPWS PW type as **ethernet** when the Ethernet interface is used to access the VPWS service.
For Kompella VPWS, only one interface can be bound in the same site mode. If an interface has been bound, other interfaces cannot be bound.
It is recommended to use the **encapsulation mpls ethernetvlan** command to set the PW encapsulation mode of the VPLS as **tag** when the subinterface is used to access the VPLS service, and set the PW encapsulation mode of the VPLS as **raw** when the Ethernet interface is used to access the VPLS service.
For the VPLS implemented by a router, a VPLS instance can bind multiple interfaces. If there are both the Ethernet interface and subinterface for access on different PEs or the same PE of one VPLS instance, it is recommended to set the VPLS PW encapsulation mode as **tag** to ensure normal interworking.
For switches, when a VLAN interface binds a VPLS service, all member interfaces of the VLAN disable the IPv4 or IPv6 multicasting function. The VLAN interface that binds the VPLS service cannot configure the subvlan, selective QinQ, mac-vlan, private-vlan, and supper-vlan functions.
The switch is bound to the SVI member interfaces of VPLS and VPWS, and the member interface type is trunk or hybrid. IPv4 or IPv6 multicast routing, igmp snooping, and mld snooping cannot be enabled on all the SVIs of these member interfaces.


Caution For switches, if the l2vpn service is accessed through the Trunk interface, it is not allowed to bind VPLS and VPWS on the default VLAN (VLAN 1).

Configuration Examples The following example binds interface gi2/2 to VPWS.

```
Ruijie(config)# l2 vfi vpls-name vpnid 25 point-to-point
Ruijie(config-vfi)# site-id 1
Ruijie(config-vfi-site)# xconnect interface gi 2/2 remote-ce-id 2
```

The following example binds interface gi2/1 to VPLS.

```
Ruijie(config)# l2 vfi vpws-name vpnid 26 autodiscovery
Ruijie(config-vfi)# site-id 1
Ruijie(config-vfi-site)# xconnect interface gi 2/1
```

Related Commands

Command	Description
ignore match l2-extcommunity	Determines whether the layer 2 extended community attribute is matched when the PW is created in Kompella mode.
show mpls vfi	Displays information of the l2vpn vfi instance.

Platform Description N/A

xconnect vfi

Use this command to enable the Martini VPLS service on the specified interface.
xconnect vfi *name*
Use the **no** form of this command to cancel the Martini VPLS service on the specified interface.
no xconnect

Parameter Description

Parameter	Description
Name	Specifies the name of the bound VFI instance.

Defaults The interface does not provide the Martini VPLS service by default.

Command Mode Interface configuration mode

Usage Guide Use this command to bind the Martini VPLS service.
For the VPLS implemented by a router, a VPLS instance can bind multiple interfaces. If there are both the Ethernet interface and subinterface for access on different PEs or the same PE of one VPLS instance, it is recommended to set the VPLS PW encapsulation mode as **tag** to ensure normal interworking. The **neighbor** command in VPLS mode can be used to specify ethernet or ethernetvlan to modify the encapsulation mode of the PW.
For switches, when a VLAN interface binds a VPLS service, all member interfaces of the VLAN disable the IPv4 or IPv6 multicasting function. The VLAN interface that binds the VPLS service cannot configure the subvlan, selective QinQ, mac-vlan, private-vlan, and supper-vlan functions.
For switches, if the l2vpn service is accessed through the Trunk interface, it is not allowed to bind VPLS and VPWS on the default VLAN (VLAN 1).
The switch is bound to the SVI member interfaces of VPLS and VPWS, and the member interface type is trunk or hybrid. IPv4 or IPv6 multicast routing, igmp snooping, and mld snooping cannot be enabled on all the SVIs of these member interfaces.

Configuration The following example binds interface gi2/2 to Martini VPLS.

Examples

```
Ruijie (config)#int gi 2/2
Ruijie (config-if)# xconnect vfi vfi1
```

Related Commands

Command	Description
ignore match l2-extcommunity	Determines whether the layer 2 extended community attribute is matched when PW is created in Kompella mode.
show mpls vfi	Displays information of the l2vpn vfi instance.

Platform Description

N/A

MPLS GR Commands

graceful-restart

Use this command to enable the graceful restart (GR) capability of LDP. Use the **no** form of this command to disable the GR capability of LDP.

graceful-restart

no graceful-restart

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the GR capability of LDP is disabled.

Command mode config-mpls-router mode

Usage Guide Use this command to enable the GR capability of LDP as follows:

- If a dual-engine device is enabled with the GR capability of LDP, traffic can be forwarded uninterruptedly and MPLS forwarding state can be consistent before and after restart when the master management board of the device becomes faulty or master/slave switchover is performed manually.
- By default, the GR capability is disabled on either of devices acting as GR-Restarter and GR-Helper.

Note The LDP session must be restarted to make the GR capability of LDP take effect.

Configuration Examples The following command enables the GR capability of LDP:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#graceful-restart
```

Related Commands

Command	Description
show mpls ldp graceful-restart	Show the LDP GR session and its parameters.

Platform Description N/A

graceful-restart timer neighbor-liveness

Use this command to configure the survival time for an LDP neighbor. Use the **no** form of this command to restore the default value.

graceful-restart timer neighbor-liveness *seconds*

no graceful-restart timer neighbor-liveness

Parameter Description

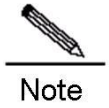
Parameter	Description
seconds	Configure the survival time for an LDP neighbor, ranging from 5s to 300s.

Defaults By default, the survival time for an LDP neighbor is 120s.

Command mode config-mpls-router mode

Usage Guide Use this command to configure the survival time for an LDP neighbor as follows:

- The device uses this value only when it acts as a GR-Helper.
- When a device acts as a GR-Helper, it selects the smaller value of the configured neighbor-liveness time and the received reconnect time to enable the survival timer and keeps "old" entries before the survival timer times out.


Note

The LDP session must be restarted to make the survival time for an LDP neighbor take effect.

Configuration Examples The following command configures the survival time for an LDP neighbor as 200s:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#graceful-restart
Ruijie(config-mpls-router)#graceful-restart timer neighbor-liveness 200
```

Related Commands

Command	Description
show mpls ldp graceful-restart	Show the LDP GR session and its parameters.

Platform Description N/A

graceful-restart timer reconnect

Use this command to configure the LDP session reconnect time. Use the **no** form of this command to

restore the default value.

graceful-restart timer reconnect *seconds*

no graceful-restart timer reconnect

Parameter Description

Parameter	Description
seconds	Configure the LDP session reconnect time, ranging from 30s to 600s.

Defaults By default, the LDP session reconnect time is 300s.

Command mode config-mpls-router mode

Usage Guide Use this command to configure the LDP session reconnect time as follows:

- During GR, both of devices acting as GR-Restarter and GR-Helper use the LDP session reconnect time.
- For the GR-Restarter, the LDP session reconnect time is used to keep "old" entries time.
- The GR-Helper selects the smaller value of the configured neighbor-liveness time and the received reconnect time to enable the survival timer and keeps "old" entries before the survival timer times out.

Note The LDP session must be restarted to make the LDP session reconnect time take effect.

Configuration Examples The following command configures the LDP neighbor reconnect time as 400s:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#graceful-restart
Ruijie(config-mpls-router)#graceful-restart timer reconnect 400
```

Related Commands

Command	Description
show mpls ldp graceful-restart	Show the LDP GR session and its parameters.

Platform Description N/A

graceful-restart timer recovery

Use this command to configure the LDP session recovery time. Use the **no** form of this command to restore the default value.

graceful-restart timer recovery *seconds*

no graceful-restart timer recovery

Parameter Description

Parameter	Description
seconds	Configure the LDP session recovery time, ranging from 15s to 600s.

Defaults By default, the LDP session recovery time is 120s.

Command mode config-mpls-router mode

Usage Guide Use this command to configure the LDP session recovery time as follows:

- The device uses this value only when it acts as a GR-Helper.
- When a device acts as a GR-Helper, it selects the smaller value of the configured recovery time and the received recovery time to enable the recovery timer and keeps "old" entries before the recovery timer times out.


Note The LDP session must be restarted to make the LDP session recovery time take effect.

Configuration Examples The following command configures the LDP session recovery time as 200s:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#graceful-restart
Ruijie(config-mpls-router)#graceful-restart timer recovery 200
```

Related Commands

Command	Description
show mpls ldp graceful-restart	Show the LDP GR session and its parameters.

Platform Description N/A

show mpls ldp graceful-restart

Use this command to show the LDP GR session and its parameters.

show mpls ldp graceful-restart [**all** | **vrf** *vrf-name*]

Parameter Description

Parameter	Description
all	Show LDP GR sessions and session parameters of all VRFs (including VRF).
vrf *vrf-name*	Show LDP GR sessions and session parameters of specified VRFs.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to show the LDP GR session and session parameter as follows:
If there is no parameter in this command, it indicates that the LDP GR sessions and session parameters of the global VRF are displayed.

Configuration Examples The following command shows the LDP GR sessions and session parameters:

```
Ruijie# show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (1 records):
    Peer LDP Ident: 20.20.20.20:0; Local LDP Ident: 10.10.10.10:0
        Status: recovering (86 seconds left)
        Address list contains 3 addresses:
          192.168.202.3   20.20.20.20    192.168.201.37
  Graceful Restart-enabled Sessions:
    Peer LDP Ident: 20.20.20.20:0, State: estab
```

Field	Description
Default VRF	Global VRF information
LDP Graceful Restart is enabled	The GR capability of LDP is enabled for a VRF.
Neighbor Liveness Timer	Survival time of the neighbor timer in the unit of second
Max Recovery Time	Maximum recovery time in the unit of second
Forwarding State Holding Time	Forwarding state holding time (reconnect time) in the unit of second
Down Neighbor Database	Down database information of an LDP neighbor
Graceful Restart-enabled Sessions	Enable LDP session information of LDP GR.
Peer LDP Ident	Peer LDP ID
State	LDP session state of an LDP neighbor

Related Commands

Command	Description
graceful-restart	Enable the GR capability of LDP.
graceful-restart timer reconnect *seconds*	Configure the reconnect time of an LDP session.
graceful-restart timer neighbor-liveness *seconds*	Configure the survival time of an LDP neighbor.

graceful-restart timer recovery *seconds*	Configure the recovery time of an LDP session.

Platform Description N/A

MPLS BFD Commands

bfd bind backward-lsp-with-ip

Use this command to configure BFD to detect whether the LSP backward link uses an IP address. Use the **no** form of this command to disable this detection function.

bfd bind backward-lsp-with-ip peer-ip *ip-address* [**vrf** *vrf-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*] **local-discriminator** *discr-value* **remote-discriminator** *discr-value*

no bfd bind backward-lsp-with-ip peer-ip *ip-address* [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
peer-ip *ip-address*	Peer IP address bound by the BFD session
vrf *vrf-name*	VRF name bound by the BFD session
interface *interface-type interface-number*	Configure the interface type and interface number.
source-ip *ip-address*	Source IP address carried by the BDF session
local-discriminator *discr-value*	Configure the local identifier of the current BFD session, ranging from 1 to 8191.
remote-discriminator *discr-value*	Configure the remote identifier of the current BFD session, ranging from 1 to 8191.

Defaults By default, this function is disabled.

Command mode Global configuration mode

Usage Guide Use this command to configure BFD to detect whether the LSP backward link uses an IP address as follows:

- If the LSP backward link uses an IP address, the forward LSP must be configured with a local identifier and a remote identifier, that is, manual configuration mode must be adopted.
- The peer IP address needs to be configured, and the source IP address is optional.
- In the case of having no specified source IP address, the source IP address in the BFD packet is not updated if the IP address of the outgoing interface is changed after the BFD session is configured successfully. In the case of having a specified source IP address, the source IP address in the BFD packet is not updated if the source IP address is changed after the BFD session is configured successfully. After the BFD session is established successfully, the identifier cannot be modified.
- The system regularly queries the BFD configuration items that sessions have been submitted but not been established and attempts to establish BFD sessions.
- The system has a limit on the number of BFD sessions. If the number of BFD sessions submitted and established by a user exceeds the upper limit allowed by the system, the system

will generate log information to prompt the user.

Configuration Examples In global configuration mode on the switch, the following command configures BFD to detect whether the LSP backward link uses an IP address. The source IP address is 20.20.20.20, and the destination IP address is 10.10.10.10. The outgoing interface is GigabitEthernet 0/2. The local identifier is 1, and the remote identifier is 2. The configuration is as follows:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport
Ruijie(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier
3
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)#bfd bind backward-lsp-with-ip peer-ip 10.10.10.10 interface
gigabitEthernet   0/2   source-ip   20.20.20.20   local-discriminator   1
remote-discriminator 2
```

Related Commands

Command	Description
bfd	Configure the parameters of the LDP session.

Platform Description N/A

bfd bind bgp-lsp

Use this command to configure BFD to detect BGP LSP. Use the **no** form of this command to remove the configuration.

bfd bind bgp-lsp peer-ip *ip-address* **source-ip** *ip-address* [**local-discriminator** *discr-value* **remote-discriminator** *discr-value*]

no bfd bind bgp-lsp peer-ip *ip-address*

Parameter description

Parameter	Description
peer-ip *ip-address*	Specifies the peer IP address.
source-ip *ip-address*	Specifies the source IP address.
local-discriminator *discr-value*	Specifies the local discriminator of BFD session, in the range from 1 to 8191.
remote-discriminator *discr-value*	Specifies the remote discriminator of BFD session, in the range from 1 to 8191.
no	Disables BFD check for BGP LSP.

Defaults BFD check for BGP LSP is disabled by default.

Command mode Global configruation mode

Usage guidelines Use this command to configure BFD to detect an BGP LSP as follows:

- This command can only be executed on ingress nodes of an LSP.
- When BFD configuration has existed, the BFD configuration item cannot be established. After BFD is configured, a BFD session starts being established immediately if the BGP LSP exists. If the BGP LSP does not exist, a BFD session starts being established when the BGP LSP exists.
- When the BGP LSP is deleted, the BFD session bound to it is deleted. However, the system reserves the configuration item of this BFD session. When the BGP LSP exists, the system re-creates a BFD session.
- The local identifier and remote identifier can be configured in a BFD session. If the local identifier is not configured, the system elects the local identifier automatically. If the LSP backward link adopts an IP address, the forward LSP must be configured with the local identifier and remote identifier manually.
- When the address of the egress of the detected LSP is borrowed or lent, the egress must be specified. Otherwise, the egress does not need to be specified.
- After a BFD session is established successfully, the identifier cannot be modified.
- The system queries regularly BFD configuration items that sessions have been submitted but not been established and attempts to establish BFD sessions.
- The system has a limitation on the number of BFD sessions. If the number of requests for establishing BFD sessions submitted by a user exceeds the limitation, the system prompts the user through log information.

Note Only BGP LSP detection established by host routes is supported.

Note One LSP can be configured with only one BFD session.

Examples Example 1: Autonegotiate an identifier.

In BGP configuration mode on the switch, configure BFD to detect BGP LSP. The source IP address is 20.20.20.20, the peer IP address is 10.10.10.10.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls ip
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#mpls ip
Ruijie(config-if-GigabitEthernet 0/2)#label-switching
Ruijie(config-if-GigabitEthernet  0/2)#bfd  interval  100  min_rx  100
```

```
multiplier 3
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)# bfd bind bgp-lsp peer-ip 10.10.10.10 source-ip 20.20.20.20
```

Example 2: Specify an identifier manually.

In LDP configuration mode on the switch, configure BFD to detect LDP LSP. The source IP address is 20.20.20.20, and the peer IP address is 10.10.10.10. The local identifier is 1, and the remote identifier is 2. The BFD session status is processed.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls ip
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#mpls ip
Ruijie(config-if-GigabitEthernet 0/2)#label-switching
Ruijie(config-if-GigabitEthernet  0/2)#bfd  interval  100  min_rx  100
multiplier 3
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)#bfd bind bgp-lsp peer-ip 10.10.10.10 source-ip 20.20.20.20
```

Related commands	**Command**	**Description**
	N/A	N/A
Platform description	N/A	

bfd bind ldp-lsp

Use this command to configure BFD to detect LDP LSP. Use the **no** form of this command to disable this function.

bfd bind ldp-lsp peer-ip *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*] **source-ip** *ip-address* [**local-discriminator** *discr-value* **remote-discriminator** *discr-value*] [**process-state**]

no bfd bind ldp-lsp peer-ip *ip-address*

Parameter Description

Parameter	**Description**
peer-ip *ip-address*	Bind the sink IP address of the LDP LSP by the BFD session.
nexthop *ip-address*	Specify the next-hop IP address of LDP LSP.
interface *interface-type interface-number*	Configure the interface type and interface number.
source-ip *ip-address*	Source IP address carried by the BFD packet
local-discriminator *discr-value*	Configure the local identifier of the current BFD session, ranging from 1 to 8191.
remote-discriminator *discr-value*	Configure the remote identifier of the current BFD session, ranging from 1 to 8191.

process-state	Process the state of the current BFD session. For some applications requiring BFD to detect faults such as delpoyments based on the cooperation BFD and LSP, this parameter is mandatory.
no	Mean disabling this function.

Defaults By default, this function is disabled.

Command mode Gloabl configuration mode

Usage Guide Use this command to configure BFD to detect an LDP LSP as follows:

- This command can only be executed on ingress nodes of an LSP.
- When BFD configuration has existed, the BFD configuration item cannot be established. After BFD is configured, a BFD session starts being established immediately if the LDP LSP exists. If the LDP LSP does not exist, a BFD session starts being established when the LDP LSP exists.
- When the LDP LSP is deleted, the BFD session bound to it is deleted. However, the system reserves the configuration item of this BFD session. When the LDP LSP exists, the system re-creates a BFD session.
- The local identifier and remote identifier can be configured in a BFD session. If the local identifier is not configured, the system elects the local identifier automatically. If the LSP backward link adopts an IP address, the forward LSP must be configured with the local identifier and remote identifier manually.
- When the address of the egress of the detected LSP is borrowed or lent, the egress must be specified. Otherwise, the egress does not need to be specified.
- After a BFD session is established successfully, the identifier cannot be modified.
- The system queries regularly BFD configuration items that sessions have been submitted but not been established and attempts to establish BFD sessions.
- The system has a limitation on the number of BFD sessions. If the number of requests for establishing BFD sessions submitted by a user exceeds the limitation, the system prompts the user through log information.

Note Only LDP LSP detection established by host routes is supported.

Note One LSP can be configured with only one BFD session.

Configuration Examples Example 1: Autonegotiate an identifier.

In LDP configuration mode on the switch, configure BFD to detect LDP LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10, and the next-hop address is 1.1.1.2. The configuration is as follows:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls ip
```

```
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport
Ruijie(config-if-GigabitEthernet 0/2)#mpls ip
Ruijie(config-if-GigabitEthernet 0/2)#label-switching
Ruijie(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier
3
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#ldp router-id interface loopback 0 force
Ruijie(config-mpls-router)#bfd bind ldp-lsp peer-ip 10.10.10.10 nexthop
1.1.1.2 source-ip 20.20.20.20
```

Example 2: Specify an identifier manually.

In LDP configuration mode on the switch, configure BFD to detect LDP LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10, and the next-hop address is 1.1.1.2. The local identifier is 1, and the remote identifier is 2. The BFD session status is processed. The configuration is as follows:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls ip
Ruijie(config)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport
Ruijie(config-if-GigabitEthernet 0/2)#mpls ip
Ruijie(config-if-GigabitEthernet 0/2)#label-switching
Ruijie(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier
3
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#ldp router-id interface loopback 0 force
Ruijie(config-mpls-router)#bfd bind ldp-lsp peer-ip 10.10.10.10 nexthop
1.1.1.2 source-ip 20.20.20.20 local-discriminator 1 remote-discriminator 2
process-state
```

Related Commands

Command	Description
bfd	Configure the parameters for the BFD session.

Platform Description N/A

bfd bind static-lsp

Use this command to configure BFD to detect a static LSP. Use the **no** form of this command to disable this function.

bfd bind static-lsp peer-ip *ip-address* **source-ip** *ip-address* [**local-discriminator** *discr-value*

remote-discriminator *discr-value*] [**process-state**]

no bfd bind static-lsp peer-ip *ip-address*

Parameter Description

Parameter	Description
peer-ip *ip-address*	Sink IP address of the static LSP bound by the BFD session
source-ip *ip-address*	Source IP address carried by the BDF packet
local-discriminator *discr-value*	Configure the local identifier of the current BFD session, ranging from 1 to 8191.
remote-discriminator *discr-value*	Configure the remote identifier of the current BFD session, ranging from 1 to 8191.
process-state	Process the state of the current BFD session. For some applications requiring BFD to detect faults such as delpoyments based on the cooperation BFD and LSP, this parameter is mandatory.

Defaults By default, this function is disabled.

Command mode Global configuration mode

Usage Guide Use this command to configure BFD to detect a static LSP as follows:

- This command can only be executed on ingress nodes of an LSP.
- When the BFD configuration has existed, the BFD configuration item cannot be established. After BFD is configured, a BFD session starts being established immediately if the static LSP exists. If the static LSP does not exist, a BFD session starts being established when the static LSP exists.
- When the static LSP is deleted, the BFD session bound to it is deleted. However, the system reserves the configuration item of this BFD session. When the static LSP exists, the system re-creates a BFD session.
- The local identifier and remote identifier can be configured in a BFD session. If the local identifier is not configured, the system elects the local identifier automatically. If the LSP backward link adopts an IP address, the forward LSP must be configured with the local identifier and remote identifier manually.
- When the address of the egress of the detected LSP is borrowed or lent, the egress must be specified. Otherwise, the egress does not need to be specified.
- After a BFD session is established successfully, the identifier cannot be modified.
- The system queries regularly BFD configuration items that sessions have been submitted but not been established and attempts to establish BFD sessions.
- The system has a limitation on the number of BFD sessions. If the number of requests for establishing BFD sessions submitted by a user exceeds the limitation, the system prompts the user through log information.

Note Only static LSP detection established by host routes is supported.

Note One LSP can be configured with only one BFD session.

Configuration Examples

Example 1: Autonegotiate an identifier.

In global configuration mode on the switch, configure BFD to detect static LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10. The configuration is as follows:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls ip
Ruijie(config)#interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport
Ruijie(config-if-GigabitEthernet 0/2)#label-switching
Ruijie(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier
3
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)#bfd bind static-lsp peer-ip 10.10.10.10 source-ip 20.20.20.20
```

Example 2: Specify an identifier manually.

In global configuration mode on the switch, configure BFD to detect static LSP. The source IP address is 20.20.20.20, the sink IP address is 10.10.10.10. The local identifier is 1, and the remote identifier is 2. The BFD session state is processed. The configuration is as follows:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls ip
Ruijie(config)#interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#no switchport
Ruijie(config-if-GigabitEthernet 0/2)#label-switching
Ruijie(config-if-GigabitEthernet 0/2)#bfd interval 100 min_rx 100 multiplier
3
Ruijie(config-if-GigabitEthernet 0/2)#exit
Ruijie(config)#bfd bind static-lsp peer-ip 10.10.10.10 source-ip 20.20.20.20
local-discriminator 1 remote-discriminator 2 process-state
```

Related Commands

Command	Description
bfd	Configure the parameters for the BFD session.

Platform Description

N/A

LDP FRR Commands

mpls ldp frr nexthop

Use this command to enable LDP FRR on interfaces. Use the **no** form of this command to remove the configuration.

mpls ldp frr nexthop *nexthop-address* [**interface** *interface-type interface-number*] [**acl** *acl-name*] [**priority** *priority*]

no mpls ldp frr nexthop { * | *nexthop-address* [**interface** *interface-type interface-number*] [**acl** *acl-name*] [**priority** *priority*] }

Parameter Description

Parameter	Description
nexthop *nexthop-address*	Specifies the next hop IP address.
interface *interface-type interface-number*	Specifies the interface type and the interface ID.
acl *acl-name*	Specifies the ACL name.
priority *priority*	Specifies the priority of the backup LSP, in the range from 1 to 65535. Default: 10. The smaller the value, the higher the priority.
nexthop *	All next hop IP addresses, i.e., all backup interfaces.

Defaults LDP FRR is disabled on the interface.

Command mode Interface configuration mode

Usage Guide

Configuration Examples The following example enabled LDP FRR on interface GE0/1:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls ip
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#label-switching
Ruijie(config-if-GigabitEthernet 0/1)#mpls ip
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#mpls ldp frr nexthop 5.5.5.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mpls ldp frr timer protect-time

Use this command to set the LDP FRR protection timer. Use the **no** form of this command to remove the configuration.

mpls ldp frr timer protect-time { **infinity** | *seconds* }

no mpls ldp frr timer protect-time

Parameter Description

Parameter	Description
infinity	When the LSP primary link fails, the traffic will never switched to the primary link.
seconds	Sets the protection timer, in the range from 0 to 65535 seconds.

Defaults The default protection timer is 10 seconds.

Command mode Interface configuration mode

Usage Guide

Configuration Examples The following example enable LDP on interface GE0/1 and sets the the LDP FRR protection timer to 15 seconds.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# mpls ip
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#label-switching
Ruijie(config-if-GigabitEthernet 0/1)#mpls ip
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)# mpls router ldp
Ruijie(config-mpls-router)#exit
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#mpls ldp frr protect-time 15
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

L3VPN FRR Commands

set vpn fast-reroute backup-next-hop

Use this command to back up the next hop on the route map. Only one next hop is allowed to be backed up. Use the **no** form of this command to remove the configuration.

set vpn fast-reroute backup-next-hop { *ip-address* **| auto** }

no set vpn fast-reroute backup-next-hop

Parameter Description

Parameter	Description
ip-address	Specifies the next hop IPv4/IPv6 address
auto	A next hop is selected for backup automatically.

Defaults No next hop is backed up by default.

Command mode Route map configuration mode

Usage Guide This command enables VPN FRR on a route map and specifies a next hop or selects the **auto** mode for next hop backup. The route map policy is based on the IP prefix list or on the ACL list.

Caution VPN FRR cannot be enabled or disabled during BGP GR.

Configuration Examples The following example creates an ACL-based route map.

```
Ruijie(config)# ip access-list standard stdacl
Ruijie(config-std-nacl)# permit host 192.168.1.2
Ruijie(config-std-nacl)# exit
Ruijie(config)# route-map routemap1 permit 10
Ruijie(config-route-map)# match ip next-hop stdacl
Ruijie(config-route-map)# set vpn fast-reroute backup-next-hop auto
```

The following example example creates an IP prefix list-based route map.

```
Ruijie(config)# ip prefix-list frrprefix  permit  1.1.1.1/32
Ruijie(config)# route-map rmp2 permit 20
Ruijie(config-route-map)# match ip next-hop prefix-list frrprefix
Ruijie(config-route-map)# set vpn fast-reroute backup-next-hop  auto
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

vpn fast-reroute route-map

Use this command to enable VPN FRR by using the route map on a VRF. Use the **no** form of this command to remove the configuration.

vpn fast-reroute route-map *route-map-name*

no vpn fast-reroute route-map

Parameter Description

Parameter	Description
route-map-name	Specifies a route map name.

Defaults This function is disabled by default.

Command mode VRF configuration mode
IPv4/IPv6 address family mode for a multi-protocol VRF

Usage Guide A troubleshooting mechanism must be configured to allow the VPN FRR to trigger active/standby switchover to protect VPN traffic.

Configuration Examples The following example enables VPN FRR by using routemap1 on vrf1:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip vrf vrf1
Ruijie(config-vrf)# vpn fast-reroute route-map routemap1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

LDP IGP SYNC Commands

mpls ldp igp sync

Use this command to enable LDP IGP synchronization ability on the interface. Use the **no** form of this command to remove the configuration.

mpls ldp igp sync

no mpls ldp igp sync

Parameter Description

Parameter	Description
N/A	N/A

Defaults LDP IGP synchronization ability is enabled on all interfaces by default.
If LDP IGP synchronization is enabled globally in OSOF routing process configuration mode, all interfaces involved in this process are enabled with LDP IGP synchronization.

Command mode Interface configuration mode

Usage Guide

- If you want to enable LDP IGP synchronization on an interface, enable LDP IGP synchronization ability on the interface first.
- If you enable LDP IGP synchronization globally by using the **mpls ldp sync** command, LDP IGP synchronization is enabled on all interfaces by default. If you want to disable LDP IGP synchronization on a specific interface, run the **no mpls ldp igp sync** command on this interface to disable its LDP IGP synchronization ability. Run the **mpls ldp igp sync** command to restore its LDP IGP synchronization ability.

Configuration Examples The following command enables LDP IGP synchronization on interface GigabitEthernet 0/1:

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no mpls ldp igp sync
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mpls ldp igp sync delay

Use this command to set the LDP IGP synchronization delay timer. Use the **no** form of this command

to remove the configuration.

mpls ldp igp sync delay *seconds*

no mpls ldp igp sync delay

Parameter Description

Parameter	Description
seconds	Sets the LDP IGP synchronization delay, in the range from 5 to 60 seconds.

Defaults LDP IGP synchronization delay is 5 seconds by default.

Command mode Interface configuration mode

Usage Guide

- After the LDP session is established, the LDP will advertise LDP convergence to IGP after the delay timer times out.
- After the LDP session is established, the LDP will not advertise LDP convergence to IGP if the LDP session is down before the delay timer timed out.
- If LDP IGP delay timer is reset when the old delay timer is running, the new timer configuration will not take effect immediately. Instead, it will take effect next time.

Configuration Examples The following examples sets the LDP IGP synchronization delay timer to 30 seconds.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mpls ldp igp sync delay 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mpls ldp igp sync holddown

Use this command to set IGP holddown timer for LDP synchronization. Use the **no** form of this command to remove the configuration.

mpls ldp igp sync holddown { *seconds* | **infinite** }

no mpls ldp igp sync holddown

Parameter Description

Parameter	Description
seconds	Sets the holddown timer, in the range from 5 to 65535 seconds.
infinite	The timer never times out, i.e., IGP waits for LDP synchronization for an infinite time.

Defaults IGP waits for LDP synchronization for an infinite time by default.

Command mode Interface configuration mode

Usage Guide The LDP IGP holddown time cannot be shorter than the LDP IGP delay. Otherwise, IGP may converge sooner than LDP.

Configuration Examples The following example sets the IGP holddown timer for LDP synchronization to 20 seconds.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mpls ldp igp sync holddown 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

mpls ldp sync

Use this command to enable LDP IGP synchronization. Use the **no** form of this command to remove the configuration.

mpls ldp sync

no mpls ldp sync

Parameter Description

Parameter	Description
N/A	N/A

Defaults LDP IGP synchronization is disabled by default.

Command mode Routing process configuration mode

Usage Guide

- Run this command in the routing process configuration mode, LDP IGP synchronization will be enabled on all OSPF-enabled interfaces.
- The OSPF routing protocol is supported while the other IGP protocols are not supported.
- A backup path must be deployed for the primary link. Otherwise, the synchronization will not take effect.

Configuration The following example enables LDP IGP synchronization.

Examples

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# mpls ldp sync
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip ospf mpls ldp interface

Use this command to show LDP IGP synchronization information on the OSPF-enabled interface. Use the **no** form of this command to remove the configuration.

show ip ospf [*process-id*] **mpls ldp interface** [*interface-name*]

Parameter Description

Parameter	Description
process-id	(Optional) Specifies a process ID.
interface-name	(Optional) Specifies an interface name.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide If no process ID is specified, interfaces involved in all OSPF processes will be shown. If no interface is specified, all interfaces will be shown.

Configuration Examples The following example shows LDP IGP synchronization information on the OSPF-enabled interface:

```
Ruijie# show ip ospf mpls ldp interface
Ethernet1/0
  Interface is up
Internet Address 1.1.10.1/24
Process ID 1, Area 0.0.0.0
SYNC Information :
Required: yes
State: sync achieved
Holddown time: infinite
Peer ident: 2.2.2.2
Send if enable
Internet Address 1.1.11.1/24
Process ID 1, Area 0.0.0.0
```

```
SYNC Information :
Required: yes
State: sync achieved
Holddown time: infinite
Peer ident: 2.2.2.2
Send if enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mpls ldp igp sync

Use this command to show LDP IGP synchronization information.

show mpls ldp igp sync [**all | vrf** *vrf-name* **| interface** *interface-name*]

Parameter Description

Parameter	Description
all	(Optional) Shows all LDP IGP synchronization information
vrf *vrf-name*	(Optional) Shows LDP IGP synchronization information on the specified VRF.
interface *interface-name*	(Optional) Shows LDP IGP synchronization information on the specified interface.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide If no VRF is specified, LDP IGP synchronization information on the global VRF will be shown.

Configuration Examples The following example shows LDP IGP synchronization information on the global VRF

```
Ruijie# show mpls ldp igp sync
Default VRF:
Ethernet0/0:
LDP configured; LDP-IGP Synchronization not enabled.
Ethernet0/1:
LDP configured; LDP-IGP Synchronization enabled.
SYNC status: sync required; achieved.
```

```
SYNC delay time: 20 seconds (10 seconds left)
IGP holddown time: infinite.
Peer LDP Ident: 20.20.20.20:0
IGP enabled: OSPF 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

MPLS ECMP Commands

ldp-ecmp

Use this command to establish equal cost LSPs for all equal cost routing FECs. Use the **no** form of this command to restore the default settings.

ldp-ecmp for all-fec

no ldp-ecmp for all-fec

Description

Parameter	Description
N/A	N/A

Default Configuration

Only the host routing FEC is established with equal cost LSP.

Command Mode

config-mpls-router mode

Usage Guide

When there are a large number of equal cost routes, establishing the equal cost LSPs only for the host routing FECs help effectively save the FIB space.

Configuration Examples

The following example establishes equal cost LSPs for all equal cost routing FECs.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls router ldp
Ruijie(config-mpls-router)# ldp-ecmp for all-fec
```

Related Commands

Command	Description
N/A	N/A

Platform Description

mpls load-balance

Use this command to configure the MPLS load balancing mode. Use the **no** form of this command to restore the default settings.

mpls load-balance { **flow | packet** }

no mpls load-balance

Description

Parameter	Description

flow	Indicates the flow-based load balancing mode.
packet	Indicates the packet-based load balancing mode.

Default Configuration

Flow-based load balancing mode is used by default.

Command Mode

config-mpls-router mode

Usage Guide

The following HASH algorithm is performed when the flow-based load balancing mode is used.

1. For MPLS flow on the P device, if the MPLS label stack is followed by the IPv4 header, use destination and source IP addresses for hash calculation and select a next hop for packet forwarding. If the MPLS label stack is not followed by the IPv4 header, use the innermost label for hash calculation and select a next hop for packet forwarding; otherwise, hash calculation is not performed and packets are forwarded to the first valid next hop.
2. For the VPWS flow on the PE device, HASH algorithm is performed using the PW label.
3. For the VPLS flow on the PE device, HASH algorithm is performed using destination MAC address and source MAC address.
3. For the L3VPN flow on the PE device, HASH algorithm is performed using destination IP address and source IP address.

Configuration Examples

The following example configures the packet-based load balancing mode.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#mpls load-balance packet
```

Related Commands

Command	Description
N/A	N/A

Platform Description

Link layer protocol Configuration Commands

HDLC Command Configurations

Configuration Related Commands

The HDLC configuration includes the following related commands:

- **encapsulation hdlc**
- **keepalive**
- **debug hdlc**

encapsulation hdlc

Use this command to encapsulate the HDLC protocol in the interface configuration mode.

encapsulation hdlc

Parameter description	None
Default	By default, HDLC is encapsulated on the RGOS synchronous interface.
Command mode	Interface configuration mode
Usage guideline	By default, HDLC is encapsulated on the RGOS synchronous interface. Therefore, this command is used only when the HDLC protocol is being encapsulated on the interface with other protocol encapsulated.

Examples	The example below encapsulates the HDLC protocol on the synchronous interface 1/0.
	`Ruijie(config)#interface serial 1/0`
	`Ruijie(config-if)#encapsulation hdlc`

keepalive

Use this command to specify the keepalive interval of sending the HDLC protocol and the maximum timeout times in the interface configuration mode. The **no** form of this command disables this function, that is, neither send the keepalive message nor process the received keepalive messages.

keepalive [*seconds* [*retries*]]
no keepalive

Parameter description

Parameter	Description
seconds	keepalive time interval, in seconds, ranging from 1-32767.
retries	Keepalive maximum timeout times, ranging from 1-255.

Default

The default keepalive interval is 10 seconds.
The default keepalive maximum timeout times are 3.

Command mode

Interface configuration mode

Usage guideline

The HDLC protocol sends a message to detect whether a link is available at a certain interval, or the keepalive time.
This command allows you to adjust the keepalive time according to link status. Be sure that keepalive time must be kept consistent at both ends of a link.

Examples

The example below specifies the HDLC keepalive time as 5 seconds, the maximum timeout times as 5

```
Ruijie(config-if)# keepalive 5 5
```

debug hdlc

Use this command to turn on the HDLC debugging switch on the synchronous interface in the privileged EXEC mode.
debug hdlc { **events** | **packets** }

Parameter description

Parameter	Description
events	HDLC event
packets	HDLC message

Default

All debugging switches are turned off by default.

Command mode

Privileged EXEC mode

Usage guideline

This command turns on the HDLC debug switch, which makes sense only when the HDLC encapsulation is enabled on the interface. **Debug Events** means turning on all HDLC event debug information, such as the HDLC keepalive message sending/receiving conditions and link statuses. The **debug packets** means turning on the HDLC message debug information, including the messages received and sent.

Examples

The example below shows the printed debug information by the RGOS when the HDLC event debug switch is turned on.

```
Ruijie#debug hdlc events
%Interface serial 1/0 : receive one HDLC keepalive packet.
%Interface serial 1/0 send one keepalive packet:
   my_seq = 21, my_seen = 20, your_seen = 16
   line protocol is UP, not in loopback state.
%Interface serial 1/0 : receive one HDLC keepalive packet.
%Interface serial 1/0 send one keepalive packet:
   my_seq = 22, my_seen = 21, your_seen = 17
   line protocol is UP, not in loopback state.
```

Where, my_seq is the sequential number of the message sent by the local end, my_seen is the sequential number of the HDLC keepalive mesage recognized by the peer end, and your_seen means the sequential number of the peer end recognized by the local end. The sequential numbers are incremental progressively.

If the my_seq is increased continuously but the my_seen and your_seen keep unchanged, it means the messages of the opposite router cannot reach the local HDLC protocol layer in the communication due to some reasons, which may be opposite device shutdown or link transmission fault. See the following debug information:

```
%Interface serial 1/0 : receive one HDLC keepalive packet.
%Interface serial 1/0 send one keepalive packet:
   my_seq = 21, my_seen = 20, your_seen = 16
   line protocol is UP, not in loopback state.
%Interface serial 1/0 send one keepalive packet:
   my_seq = 22, my_seen = 20, your_seen = 16
   line protocol is UP, not in loopback state.
%Interface serial 1/0 send one keepalive packet:
   my_seq = 23, my_seen = 20, your_seen = 16
   line protocol is UP, not in loopback state.
```

PPP and MP Configuration Commands

debug ppp

Use this command to turn on the PPP negotiation debugging switch in the privileged EXEC mode.
debug ppp [authentication|error|multilink|negotiation|packet]

Parameter description

Parameter	Description
authentication	ppp authentication
error	ppp negotiation error
multilink	ppp multilink
negotiation	ppp negotiation process
packet	ppp negotiation message

Default configuration

If the debugging option is not specified, the PPP authentication is turned on by default.

Command mode

Privileged EXEC mode

Usage guideline

This command is mostly used to trace the process of PPP negotiation. In actual applications, it is possible to turn on different debug switches as required.

Examples

The example below turns on the authentication debugging switch.

```
Ruijie#debug ppp authentication
Ruijie# show debug
Ruijie# show debugging
   ppp:
PPP authentication debugging is on
```

encapsulation ppp

Use this command to encapsulate the PPP protocol on the interface. The **no** form of this command disables the PPP encapsulation.
encapsulation ppp
no encapsulation

Parameter description	None
Default	HDLC encapsulation is enabled on the synchronous interface and no encapsulation is enabled on the asynchronous interface by default
Command mode	Interface configuration mode

Examples	The example below configures PPP on the synchronous interface 0.
	`Ruijie(config)#interface serial 0`
	`Ruijie(config-if)#encapsulation ppp`

interface dialer

Use this command to create a dialup interface for multilink dialup. The **no** form of this command deletes the specified logical interface.

interface dialer *group-number*

no interface dialer *group-number*

Parameter description

Parameter	Description
group-number	Number of the dialup interface (also called the rotary group number), one-to-one corresponding to the **rotary-group** command option **number**.

Default	No logical interface created
Command mode	Global configuration
Usage guideline	To implement the multilink connection in dialup mode, you need to create a dialup logical interface by using this command and then use the **dialer rotary-group** command to bind the physical interface prepared for the multilink connections to that dialup logical interface. The specific communication parameters of multilink are negotiated on the logical interface.
Examples	The example below creates a logical interface, numbered as 0. `Ruijie(config)#interface dialer 0`

Related commands	Command	Description
	dialer rotary-group	Bind the physical interface to the specified dialup interface

interface multilink

Use this command to create a multilink interface for multilink operation. The **no** form of this command deletes the specified multilink interface.

interface multilink *group-number*

no interface multilink *group-numbe*

Parameter description	Parameter	Description
	group-number	Number of the multilink interface (also called the group number), one-to-one corresponding to the **ppp multilink group** command option **group-number**.

Default	No logical interface created
Command mode	Global configuration
Usage guideline	To implement the multilink connection in non-dialup mode, it is required to create a multilink logical interface by using this command and then use the **ppp multilink group** command to bind the physical interface prepared for the multilink connections to that multilink logical interface. The specific communication parameters of multilink are set in the logical interface.
Examples	The example below creates a logical interface, numbered as 0. `Ruijie(config)#interface multilink 0`

Related commands	Command	Description
	ppp multilink group *group-number*	Bind the physical interface to the specified multilink interface

multilink bundle-name

Use this command to specify the naming method for MP bundle. The **no** form of this command cancels the related method.

multilink bundle-name {**authenticated** | **endpoint** | **both**}

no multilink bundle-name

Parameter description

Parameter	Description
authenticated	Opposite authentication name, default setting
endpoint	Opposite endpoint descriptor
both	Opposite authentication name and endpoint descriptor

Default

Opposite authentication name

Command mode

Global configuration

Usage guideline

The keyword **authenticated** specifies the named bundle of the opposite authentication name. If no authentication is required, the opposite endpoint descriptor is used. If no authentication or endpoint descriptor is available, the calling party ID will be used.

The keyword **endpoint** specifies the named bundle of the opposite endpoint descriptor. If no endpoint descriptor is available, the opposite authentication name is used. If no authentication or endpoint descriptor is available, the calling party ID will be used.

The keyword **both** specifies the named bundle of the opposite authentication name + endpoint descriptor. If no endpoint descriptor is available, the opposite authentication name is used. If no authentication name is available, the endpoint descriptor is used. If no authentication or endpoint descriptor is available, the calling party ID will be used.

Examples

The example below specifies the named bundle of the opposite endpoint descriptor:

```
Ruijie(config)#multilink bundle-name endpoint
```

multilink virtula-template

Use this command to specify the MP bundle interface to be able to have the virtual template of its clone interface parameters. The **no** form of this command cancels the definition of virtual template.

multilink virtual-template *number*

no multilink virtual-template

Parameter description

Parameter	Description
number	Virtual template interface number, range 1 ~ 1200.

Default

No template number defined

Command mode

Global configuration

Usage guideline

Configuring a specified IP address on the virtual template may result in the establishment of an incorrect route, causing loss of IP messages.

Examples

The example below specifies using the MP virtual template and applying it on an MP bundle interface:

```
Ruijie(config)#multilink virtual-template 1
Ruijie(config)#interface virtual-template 1
Ruijie(config-if)#ip unnumbered fastEthernet 0/0
Ruijie(config-if)#encapsulation ppp
Ruijie(config-if)#ppp multilink
Ruijie(config-if)#ppp authentication chap
```

Related commands

Command	Description
interface virtual-template	Create the virtual template interface

ppp aaa-auth ignore framed-ip

Use this command to set the framed-ip-address to 0 during AAA authentication to ensure compatibility between the router and some AAA servers. Use the **no** form of this command to restore the default setting.

ppp aaa-auth ignore framed-ip

no ppp aaa-auth

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This command is not configured by default.

Command Mode Interface configuration mode

Usage Guide This command is valid and displayed only in AAA authentication mode

Configuration Examples The following example sets the framed-ip-address to 0 during AAA authentication.

```
Ruijie(config)#aaa new-model
Ruijie(config)#
Ruijie(config)#int virtual-template 1
Ruijie(config-if-Virtual-Template 1)#ppp aaa-auth ignore framed-ip
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp acfc local

Use this command to configure how the local router processes the ACFC option in the to-be-sent PPP configuration request. Use the **no** form of this command to restore the default setting.

ppp acfc local { **request** | **forbid** }

no ppp acfc local

Parameter Description	Parameter	Description
	request	Initiates ACFC negotiation on the local end, that is, the PPP LCP request packet to be sent from the local end carries the ACFC option
	forbid	Forbids ACFC negotiation on the local end, that is, the PPP LCP request packet to be sent from the local end does not carry the ACFC option and the request packet that carries the ACFC option and that is sent from the peer end is rejected.

Defaults If the interface is an AYSNC interface, the ACFC option is contained in the request packet.
If the interface is not an AYSNC interface, the ACFC option is not contained in the request packet and the local end rejects the ACFC option contained in the request packet from the peer end.

Command Mode Interface configuration mode

Usage Guide If the **ppp acfc local** command conflicts with the **ppp acfc remote** command, the later configured command shall prevail.

Configuration Examples The following example contains the ACFC option in the request packet sent from the local end.

```
Ruijie(config)# interface serial 3/1
Ruijie(config-if)# ppp acfc local request
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ppp acfc remote

Use this command to configure how the local router processes the PPP configuration request packet that carries the ACFC option and that is sent from the remote device. Use the **no** form of this command to restore the default setting.

ppp acfc remote { **apply** | **reject** | **ignore** }

no ppp acfc remote

Parameter Description

Parameter	Description
apply	Accepts ACFC negotiation from the peer end. That is, ACFC is enabled for PPP frames from the peer end, but is enabled or disabled for PPP frames from the local end based on the interface type.
reject	Rejects ACFC negotiation from the peer end.
ignore	Ignores ACFC negotiation from the peer end. That is, ACFC can be enabled or disabled for PPP frames from the peer end, but is disabled for PPP frames from the local end.

Defaults If an interface is an ASYNC interface, it accepts the ACFC option by default. Otherwise, the ACFC option is rejected.

Command Mode Interface configuration mode

Usage Guide If the **ppp acfc local** command conflicts with the **ppp acfc remote** command, the later configured command shall prevail.

Configuration Examples The following example accepts the ACFC option in the request packet sent from the peer end. Whether the PPP frame sent from the local end applies the ACFC option depends on the interface type.

```
Ruijie(config)# interface async 1
```

```
Ruijie(config-if)# ppp acfc remote apply
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp authentication

Use this command to implement the PPP authentication on the interface. To enable the AAA security service, use this command to associate the authentication method list. The **no** format of this command cancels the association and restores the default.

ppp authentication {**chap**|**pap**|**chap pap|pap chap}** [**callin**]

no ppp authentication {**chap**|**pap**}

Parameter description

Parameter	Description
chap	Enable the CHAP authentication on the interface
pap	Enable the PAP authentication on the interface
char pap	Enable the CHAP and PAP authentication at the same time. Perform CHAP authentication before the PAP authentication.
pap chap	Enable the CHAP and PAP authentication at the same time. Perform PAP authentication before the CHAP authentication.
callin	Allow the unidirectional CHAP or PAP authentication only when the opposite end acts as the dialup end. This parameter is used for the asynchronous dialup interface. The current version of the RGOS does not support the synchronous interface used for the purpose of asynchronous interface. This parameter is used for the compatible interface.

Default The ppp authentication defines the default method list, and PPP authentication is used by using the local database.

Command mode	Interface configuration mode
Usage guideline	This command defines the PPP authentication method, by using the local user database. Caution: With the ppp authentication chap pap configured on the authentication server, the Ruijie's router which acts as the client uses the chap mode by default.

Examples	The example below enables CHAP authentication on the asynchronous interface 1.
	`Ruijie(config)#int async 1`
	`Ruijie(config-if)#ppp authentication chap`

Related commands

Command	Description
aaa authentication ppp	Define the PPP authentication method list
aaa new-model	Enable the AAA security service
encapsulation ppp	Encapsulate PPP
username	Define a local user database

ppp chap hostname

Use this command to specify the hostname for the CHAP authentication. The **no** format of this command restores the default hostname.

ppp chap hostname *hostname*

no ppp chap hostname

Parameter description

Parameter	Description
hostname	Hostname sent in the CHAP authentication

Default	The name of the router is used in any CHAP authentication.
Command mode	Interface configuration mode

Usage guideline	In an ever-expanding network, it is required to configure the newly-added username/password pair on every router that participates in the authentication, resulting in large efforts of the modification. If the **ppp chap hostname** is used to define the common host alias for CHAP authentication, only one username/password pair is needed on every router, which eliminates the huge configuration efforts of username/password pairs.

Examples	The example below specifies the CHAP authentication hostname as comhost on the asynchronous interface 1.
	`Ruijie(config)#int async 1`
	`Ruijie(config-if)#ppp chap hostname comhost`

Related commands

Command	Description
aaa authentication ppp	Define AAA PPP authentication method list
ppp authentication	Configuring the ppp authentication mode
ppp chap password	Configure the CHAP authentication common password

ppp chap password

Use this command to configure the common CHAP authentication password. The **no** form of this command cancels the CHAP authentication common password.

ppp chap password *[encryption-type] secret*

no ppp chap password

Parameter description

Parameter	Description
encryption-type	Encryption type for the password message
secret	CHAP authentication common password

Default	No common password
Command mode	Interface configuration mode

Usage guideline	Just like the common hostname configured with the **ppp chap hostname** command, the **ppp chap password** also aims to keep the existing network device configurations for the CHAP authentication in an ever-expanding network. The difference is that the **ppp chap password** is used to define the common CHAP authentication password and enable the authentication without knowing the opposite hostname.

Examples	The example below specifies the common password **comword** for the CHAP authentication.
	`Ruijie(config)#int as 1`
	`Ruijie(config-if)#ppp chap password 0 comword`

Related commands

Command	Description
aaa authentication ppp	Define AAA PPP authentication method list.
ppp authentication	Configure the ppp authentication mode.
ppp chap hostname	Configure the CHAP authentication common hostname.

ppp chap refuse

Use this command to reject the CHAP authentication initiated by the peer end. Use the **no** form of this command to restore the default setting.

ppp chap refuse

no ppp chap refuse

Parameter Description

Parameter	Description
N/A	N/A

Defaults This command is not configured by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example configures AYSNC interface 1 to reject the CHAP authentication initiated by the peer end.

```
Ruijie(config)# int async 1
Ruijie(config-if)# encapsulation ppp
```

```
Ruijie(config-if)# ppp chap refuse
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp lcp accept-option

Use this command to identify the PPP LCP extended configuration option from the peer end and send the information in the extended configuration option to the AAA server. Use the **no** form of this command to restore the default setting.

ppp lcp accept-option

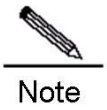
no ppp lcp accept-option

Parameter Description	Parameter	Description
	N/A	N/A

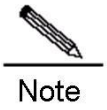
Defaults The PPP LCP extended configuration option is not identified.

Command Mode Interface configuration mode

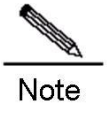
Usage Guide



Run the **ppp lcp accept-option** command to identify the PPP LCP extended configuration option from the peer end carrying IMSI number, the SN or the MAC address.



In addition to the **ppp lcp accept-option** command, run the **force-local-lcp** command on the LNS device to transmit the IMSI, the SN, or the MAC address via the PPP LCP extended configuration option. In addition, the functions must be normal to ensure that the IMSI/MAC/SN extended configuration option is identified.



The LAC device of the ISP may not support LCP re-negotiation and the configuration of the **force-local-lcp** command will result in a PPP negotiation failure. As a result, the IMSI/MAC/SN authentication function is unavailable.

Configuration Examples The following example receives the PPP LCP extended configuration option and sends the information in the extended configuration option to the AAA server

```
Ruijie(config)# interface virtual-template 1
```

```
Ruijie(config-if)# ppp lcp accept-option
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp lcp send-option

Use this command to send the LCP extended configuration option carrying the IMSI number, the SN, or the MAC address to the peer end. Use the **no** form of this command to restore the default setting.

ppp lcp send-option { **imsi** | **serial-number** | **mac-address** }

no ppp lcp send-option { **imsi** | **serial-number** | **mac-address** }

Parameter Description	Parameter	Description
	imsi	IMSI
	serial-number	Router SN
	mac-address	MAC address

Defaults The PPP LCP extended configuration option is not sent.

Command Mode Interface configuration mode

Usage Guide Run the **ppp lcp send-option** command to identify the PPP LCP extended configuration option carrying IMSI number, the SN or the MAC address.

Configuration Examples The following example sends the LCP extended configuration option carrying the SN to the peer end.

```
Ruijie(config)# interface dialer 1
Ruijie(config-if)# ppp lcp send-option serial-number
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp ms-chap refuse

Use this command to reject the MS CHAP authentication initiated by the peer end. Use the **no** form of this command to restore the default setting.

ppp ms-chap refuse

no ppp ms-chap refuse

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This command is not configured by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example configures AYSNC interface 1 to reject the MS CHAP authentication initiated by the peer end.

```
Ruijie(config)# int async  1
Ruijie(config-if)# encapsulation ppp
Ruijie(config-if)# ppp ms-chap refuse
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp ms-chap-v2 refuse

Use this command to reject the MS CHAP v2 authentication initiated by the peer end. Use the **no** form of this command to restore the default setting.

ppp ms-chap-v2 refuse

no ppp ms-chap-v2 refuse

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This command is not configured by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example configures AYSNC interface 1 to reject the MS CHAP v2 authentication initiated by the peer end.

```
Ruijie(config)# int async  1
Ruijie(config-if)# encapsulation ppp
```

```
Ruijie(config-if)# ppp ms-chap-v2 refuse
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp multilink

Use this command to enable the PPP multilink on the interface. The **no** format of this command disables the PPP multilink function.

ppp multilink

no ppp multilink

Parameter description	None
Default configuration	The PPP multilink function is not enabled
Command mode	Interface configuration mode
Usage guideline	This command is generally used in the logical interface with DDR kept, used for multilink dialup. When the PPP multilink is enabled, the router first stimulates the first channel dialup. When the load of the current link reaches the threshold set by the **dialer load-threshold**, it enables the idle lines for dialup. If the total load of the current link is below the threshold, the idle line will be disconnected. (In this case, this line must not be the only available one at present.) During the process of multilink dialup, full PPP negotiation is performed for the first channel dialup, and only LCP and multilink negotiation is performed for the subsequential dialup.

Examples	The example below enables the PPP multilink on logical interface 1.
	`Ruijie(config)#int d 1`
	`Ruijie(config-if)#ppp multilink`

Related commands	Command	Description
	ppp authentication	Configure the PPP authentication.
	dialer load-threshold	Specify the load threshold of the line.

encapsulation ppp	Encapsulate PPP.
dialer idle-timeout	Specify the idle time of the line.

ppp multilink endpoint

Use this command to change the system default endpoint descriptor. The **no** form of this command restores the default endpoint descriptor.

ppp multilink endpoint {hostname | ip *ip-address* **| mac** *lan-interface* **| none | phone** *telephone-number* **| string** *char-string***}**

no ppp multilink endpoint

Parameter description

Parameter	Description
hostname	Specify the host name.
ip ip-address	IP address
mac *lan-interface*	Specify the MAC address.
none	Endpoint descriptor is not negotiated
phone *telephone-number*	Specify the telephone number
string *char-string*	Specify the character string

Default configuration

Hostname in the global configuration mode, or the hostname configured with **chap hostname** in the interface configuration mode, or the username configured with **pap sent-username**

Command mode

Interface configuration mode

Usage guideline

By default, the PPP uses the same string as the endpoint descriptor to negotiate the MP. This string is set with the **ppp chap hostname** or **ppp pap sent-username** command in the interface configuration mode or the **hostname** command in the global configuration mode. The **ppp multilink endpoint** command configures the custom endpoint descriptor . The **no** format of this command restores the default.

The **no ppp multilink endpoint** command differs from the **ppp multilink endpoint hostname** command as follows: the former allows the use of authentication name (which can be the hostname, or not) while the latter specifies using the hostname of the router.

The parameters **hostname** and **string** use the local endpoint descriptors of the same kind. The difference between them is that the

former allows entering custom value while the latter uses the router hostname.

Do not use this command on the MP bundle interface. It shall be used on every interface that may become a member of the MP bundle.

Examples

The example below uses the IP address 10.1.1.4, instead of the CAHP specified hostname group 1, as the endpoint descriptor:

```
Ruijie(config)#interface dialer0
Ruijie(config-if)#ip address 10.1.1.4 255.255.255.0
Ruijie(config-if)#encapsulation ppp
Ruijie(config-if)#dialer remote-name R-name
Ruijie(config-if)#dialer string 23456
Ruijie(config-if)#dialer pool 1
Ruijie(config-if)#dialer-group 1
Ruijie(config-if)#ppp chap hostname group 1
Ruijie(config-if)#ppp multilink endpoint ip 10.1.1.4
```

Related commands

Command	Description
multilink bundle-name	Specify the MP bundle method.
ppp chap hostname	Specify the hostname for CHAP authentication.
ppp pap sent-username	Specify the username and password requested for PAP authentication.

ppp multilink fragment delay

Use this command to specify the maximum size of the fragment measured by delay in an MP bundle. The **no** format of this command restores the default maximum delay.

ppp multilink fragment delay *delay-max*

no ppp multilink fragment

Parameter description

Parameter	Description
delay-max	Maximum delay, in milliseconds, range 1 - 1000 milliseconds

Default configuration

No default for the fragment size; 30 milliseconds for the maximum delay of the MP fragment

Command mode

Interface configuration mode

Usage guideline

By default, no fragment is specified for the MP, and the MP performs fragmentation for messages according to the number of channels in the bundle. The size of the fragment is not limited, and the maximum number of fragments is limited by the number of channels. If different bandwidths are available for the channels in the bundle or the **ppp multilink fragment delay** command is set, the MP uses different fragmentation algorithms. In this case, the number of the fragments will not be limited but the size of each fragment will be limited by the fragment delay time. If no fragment delay is configured, this delay time is 30 milliseconds by default.

The **ppp multilink fragment delay** command can be used when it is required to control the traffic characteristics such as delay and load balancing.

The MP converts the delay time delay-max into size of bytes according to the speed of each channel. If the channels in the bundle have different speeds, the fragments of the channels will be different.

By default, the system fragment delay time is 30 milliseconds. For the three commands **ppp multilink fragment delay**, **ppp multilink fragment maximum** and **ppp multilink fragment size**, only one policy can be used at one time, so the one configured at last will take effective. If only one command is configured, the values of the other two will be cancelled.

Caution If the **ip ref** command has been configured on the interface, this command will not take effect.

Examples

The example below specifies the maximum delay time of the interface as 20 milliseconds.

```
Ruijie(config-if)#ppp multilink fragment delay 20
```

Related commands

Command	Description
ppp multilink	Enable the MP on the interface.
ppp multilink fragment disable	Enable/disable fragment.
ppp multilink fragment maximum	Specify the number of fragmented messages.
ppp multilink fragment size	Specify the size of fragmented messages.

ppp multilink fragment disable

Use this command to disable the message fragment. The **no** format of this command restores the message fragment.

ppp multilink fragment disable

no ppp multilink fragment

Parameter description	None
Default configuration	Message fragment is enabled.
Command mode	Interface configuration mode
Usage guideline	If the fragment causes decrease of execution efficiency, this command can be used to disable it. If it is noticed that the channels are not synchronized, it means the fragment causes decrease of efficiency. This command does not forbid fragment completely. If fragment becomes necessary, such as the size of message in the bundle exceeding the MTU size of the channel, the fragment will be implemented.
Examples	The example below disables fragment. `Ruijie(config-if)#ppp multilink fragment disable`

Related commands

Command	Description
ppp multilink fragment delay	Specify the message fragment delay
ppp multilink fragment maximum	Specify the maximum number of fragmented messages
ppp multilink fragment size	Specify the size of fragmented messages

ppp multilink fragment maximum

Use this command to specify the maximum number of the fragments in an MP bundle. The **no** form of this command restores the default maximum number of fragments.

ppp multilink fragment maximum *fragments*

no ppp multilink fragment

Parameter description

Parameter	Description
fragments	Maximum number of fragments, range: 2-8

Default configuration

N/A

Command mode

Interface configuration mode

Usage guideline

This command controls how many fragments can be produced in a message.

If you want to limit the number of fragment instead of its size, run this command. For more discussions on fragment, see the guide to the **ppp multilink fragment delay** commands.

Examples

The example below specifies the maximum four fragments of a message.

```
Ruijie(config-if)#ppp multilink fragment maximum 4
```

Related commands

Command	Description
ppp multilink fragment delay	Specify the message fragment delay
ppp multilink fragment disable	Enable/disable fragment
ppp multilink fragment size	Specify the size of fragmented messages

ppp multilink fragment size

Use this command to set the size of a fragment for multilink. The **no** form of this command restores default.

ppp multilink fragment size *bytes*

no ppp multilink fragment

Parameter description

Parameter	Description
bytes	Size of fragment

Default configuration	No settings for the command by default
Command mode	Interface configuration mode
Usage guideline	By default, no fragment is specified for the MP, and the MP performs fragmentation for messages according to the number of channels in the bundle. There is no restriction to the size of the fragment. If different bandwidths are available for the channels in the bundle or the **ppp multilink fragment delay** command is set, the MP uses different fragmentation algorithms. In this case, the size of fragments will be limited. The ppp multilink fragment delay command can be used when it is required to control the traffic characteristics such as delay and load balancing. The **ppp multilink fragment maximum** command can be used when it is required to control the characteristics of maximum number of fragments. If the **ppp multilink fragment size** command is used, the MP messages will be divided into fragments of specified size.
Examples	The example below specifies the size of message fragment as 128 bytes. `Ruijie(config-if)#`**`ppp multilink fragment size`** *`128`*

Related commands

Command	Description
ppp multilink fragment delay	Specify the message fragment delay
ppp multilink fragment disable	Enable/disable fragment
ppp multilink fragment size	Specify the size of fragmented messages

ppp multilink group

Use this command to add the physical link into the specified multilink-group interface. The **no** form of this command removes the physical interface from the bundle.

ppp multilink group *group-number*

no ppp multilink group

Parameter description

Parameter	Description
group-number	multilink-group interface number (non-zero)

Default configuration

No settings for the command by default

Command mode

Interface configuration mode

Usage guideline

There is no setting for this command by default, which means it is possible to add the channel into any bundle in the system through negotiation.

If the command is set, the physical channel is limited and can be only added into the specified multilink-group interface. If the opposite end of the channel attempts to join a different bundle, the connection will be limited. This command is used when the local party and the opposite party are negotiating the MP.

Examples

The example below specifies adding the synchronous interface 0/1 into multilink bundle 1:

```
Ruijie(config)#interface serial 0/1
Ruijie(config-if)#encapsulation ppp
Ruijie(config-if)#ppp multilink group 1
Ruijie(config-if)#ppp multilink
Ruijie(config-if)#ppp authentication chap
```

Related commands

Command	Description
interface multilink	Create a multilink interface and enter into the multilink interface configuration mode.

ppp multilink links maximum

Use this command to specify the maximum number of channels in an MP bundle. The **no** form of this command restores default.

ppp multilink links maximum *links*

no ppp multilink links maximum

Parameter description

Parameter	Description
links	Maximum number of channels, range 1 - 64

Default configuration	16
Command mode	Interface configuration mode
Usage guideline	This command specifies the maximum number of channels allowed in a bundle. When more channels attempt to join the bundle, the MP disconnects the dialup communication to reduce the number of bundles. If the channels do not correspond to a dialup line, they will not be affected by this command. If the bundle is mixed with lease lines and dialup lines, the lease lines will keep permanent connection even when the number of lease lines exceeds the maximum number of bundles. This command works with the **PPP multilink load-threshold** command to prevent enabling a good many of channels in case a low traffic load threshold has been set.
Examples	The example below specifies the maximum number of channels as 50: `Ruijie(config-if)#ppp multilink links maximum 50`

Related commands

Command	Description
ppp multilink links minimum	Specify the minimum number of channels in an MP bundle.

ppp multilink links minimum

Use this command to specify the minimum number of channels in an MP bundle. The **no** form of this command restores default.

ppp multilink links minimum *links*

no ppp multilink links minimum

Parameter description

Parameter	Description
links	Minimum number of channels, range 0 - 64

Default configuration	0
Command mode	Interface configuration mode
Usage guideline	If the number of channels in a bundle is less than the setting value with this command and there are available channel that can be enabled (such as the dialup lines available), MP will attempt to enable the channels till it reaches the setting value. If the **ppp multilink links maximum** is set, MP will not make the number of channels bigger than the value set by the former even if the value set with the **ppp multilink links minimum** command is bigger than it. This command takes effect only for the channels with connections established. This command limits the minimum number of channels that attempt to keep connection by the MP in a bundle. Even if the traffic does not exceed the load threshold, MP will attempt dial up to add lines to make the number of channels reach the setting value. This command is used only in the dynamic broadband environment with dialup on demand.
Examples	The example below specifies the minimum number of channels as 12: `Ruijie(config-if)#ppp multilink links minimum 12`

Related commands

Command	Description
ppp multilink links maximum	Specify the maximum number of channels in an MP bundle.

ppp multilink load-threshold

Use this command to make the MP monitor the traffic load and adjust the bandwidth through dialup according to the change of loads. The **no** form of this command cancels this function.

ppp multilink load-threshold *load-threshold* {**outbound|inbound|either**}

no ppp multilink load-threshold

Parameter description

Parameter	Description
load-threshold	Add or delete channel load threshold, range 1 - 255. 255 means 100% load. 1 means any

		load. When 1 is set, the MP ignores the actual traffic load and enables channels as many as possible.
	outbound	Monitor outgoing traffic only.
	inbound	Monitor incoming traffic only.
	either	Monitor incoming and outgoing traffic at the same time. The change of load in any direction may cause the connection/disconnection of the channel.

Default configuration	The function is not enabled by default. If no optional parameter is entered, the outgoing traffic will be monitored by default.
Command mode	Interface configuration mode
Usage guideline	Generally, the **dialer load-threshold** command rather than the **ppp multilink load-threshold** command is used. When the bundle is configured from a dialup interface, the MP inherits the setting value with the **dialer load-threshold**.
Examples	The example below sets the incoming load threshold of MP as 10: `Ruijie(config-if)#ppp multilink load-threshold 10 inbound`

Related commands	**Command**	**Description**
	dialer load-threshold	Specify the maximum load.
	ppp multilink links maximum	Specify the maximum number of channels in a bundle.
	ppp multilink links minimum	Specify the minimum number of channels in a bundle.

ppp negotiation-timeout

Use this command to set the PPP negotiation timeout. The **no** form of this command restores default.

ppp negotiate-timeout *seconds*
no ppp negotiate-timeout

Parameter description	

Parameter	Description
seconds	Timeout period, in seconds

Default	The default is 20 seconds.
Command mode	Interface configuration mode
Usage guideline	During the PPP negotiation, both LCP and IPCP have timeout periods. Once the period expires, the LCP resends requests. This period can be set by using this command to coordinate the negotiation time in the interconnection with heterogeneous devices.
Examples	The example below specifies the PPP negotiation period as 10 seconds. `Ruijie(config-if)#`**`ppp negotiation-timeout`** *`10`*

ppp pap refuse

Use this command to reject the PAP authentication initiated by the peer end. Use the **no** form of this command to restore the default setting.

ppp pap refuse

no ppp pap refuse

Parameter Description	Parameter	Description
	N/A	N/A

Defaults	This command is not configured by default.
Command Mode	Interface configuration mode
Usage Guide	N/A
Configuration Examples	The following example configures AYSNC interface 1 to reject the PAP authentication initiated by the peer end.

```
Ruijie(config)# int async  1
Ruijie(config-if)# encapsulation ppp
Ruijie(config-if)# ppp pap refuse
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

ppp pap sent-username

Use this command to configure the support for remote PAP authentication. The **no** form of this command cancels the support for the remote PAP authentication.

ppp pap sent-username *username* **password** *[encryption-type] password*

no ppp pap sent-username

Parameter description

Parameter	Description
usename	Username sent in the PAP authentication
encryption-type	Encryption type of the password sent in the PAP authentication
password	Password sent in the PAP authentication

Default The username and password of the local router are not sent.

Command mode Interface configuration mode

Usage guideline If the remote router performs the PAP authentication for the local router, it is required to use the **ppp pap sent-username** command on the local router to define the username and password sent in the PAP authentication.

Examples The example below specifies the username papuser and password pappassword sent for the PAP authentication.

```
Ruijie(config)#int as 1
Ruijie(config-if)#ppp pap sent-username papuser password 0 pappassword
```

Related commands

Command	Description
aaa authentication ppp	Define AAA PPP authentication method list
ppp authentication	Configure the PPP authentication mode.

ppp chap hostname	Configure the CHAP authentication common hostname.
ppp chap password	Configure the CHAP authentication common password.

ppp pfc local

Use this command to configure how the local router processes the PFC option in the to-be-sent PPP configuration request. Use the **no** form of this command to restore the default setting.

ppp pfc local { **request** | **forbid** }

no ppp pfc local

Parameter Description

Parameter	Description
request	Initiates PFC negotiation on the local end, that is, the PPP LCP request packet to be sent from the local end carries the ACFC option
forbid	Forbids PFC negotiation on the local end, that is, the PPP LCP request packet to be sent from the local end does not carry the PFC option and the request packet that carries the ACFC option and that is sent from the peer end is rejected.

Defaults

If the interface is an AYSNC interface, the PFC option is contained in the request packet.

If the interface is not an AYSNC interface, the PFC option is not contained in the request packet and the local end rejects the PFC option contained in the request packet from the peer end.

Command Mode

Interface configuration mode

Usage Guide

If the **ppp pfc local** command conflicts with the **ppp pfc remote** command, the later configured command shall prevail.

Configuration Examples

The following example contains the PFC option in the request packet sent from the local end.

```
Ruijie(config)# interface serial 3/1
Ruijie(config-if)# ppp pfc local request
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ppp pfc remote

Use this command to configure how the local router processes the PPP configuration request packet that carries the PFC option and that is sent from the remote device. Use the **no** form of this command to restore the default setting. Use the **no** form of this command to restore the default setting.

ppp pfc remote { **apply** | **reject** | **ignore** }

no ppp pfc remote

Parameter Description

Parameter	Description
apply	Accepts PFC negotiation from the peer end. That is, PFC is enabled for PPP frames from the peer end, but is enabled or disabled for PPP frames from the local end based on the interface type.
reject	Rejects PFC negotiation from the peer end.
ignore	Ignores PFC negotiation from the peer end. That is, PFC can be enabled or disabled for PPP frames from the peer end, but is disabled for PPP frames from the local end.

Defaults If an interface is an ASYNC interface, it accepts the PFC option by default. Otherwise, the PFC option is rejected.

Command Mode Interface configuration mode

Usage Guide If the **ppp pfc local** command conflicts with the **ppp pfc remote** command, the later configured command shall prevail.

Configuration Examples The following example accepts the PFC option in the request packet sent from the peer end. Whether the PPP frame sent from the local end applies the PFC option depends on the interface type.

```
Ruijie(config)# interface async 1
Ruijie(config-if)# ppp pfc remote apply
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show interfaces

Use this command to show the PPP information of the interface.

show interface *[type slot-number/interface-number]*

Parameter description

Parameter	Description
type	Type of the interface
slot-number	Number of the slot of the specific interface
interface-number	Number of the port of the specific interface

Command mode

Privileged EXEC mode

Usage guideline

This command is used to view the parameter statistics during the process of PPP negotiation.

username

Use this command to set the local user database.

username*name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*]

username *name* **password** *secret*

username *name* [**privilege** *level*]

Parameter description

Parameter	Description
name	Hostname, server name, user ID or command name. The parameter **name** can be one word only. No space or question mark is allowed.
nopassword	No login password is used for the user. It generally works with the keyword **autocommand**.
password	Specify password for the user.
password	Specify the possible password text for the user.
encryption-type	Encryption type: The encryption type 0 means no encryption for the text that closely follows it; the encryption type 7 means the text that closely follows it is encrypted.
encrypted-password	Encryption password entered by the user.
password	Specify password for the user.

	secret	Encryption password entered by the user.
	privilege	Set the privilege level for the user
	level	A number between 0 and 15, specifying the privilege level of the user

Default	No local user database is built by default.
Command mode	Global configuration mode
Usage guideline	This command is used to establish local user database for the purpose of authentication. In addition to the username and password, this command can also specify more options (such as callback) for some additional actions. However, it can specify some simple actions. For more complex settings, the security server has to be used instead.
Examples	The example below creates a username/password pair. `Ruijie(config)#username red password 0 redpw`

Frame Relay Configuration Commands

Configuration Related Commands

The frame relay configuration involves the following related commands:
debug frame-relay
clear frame-relay-inarp
encapsulation frame-relay
frame-relay interface-dlci
frame-relay intf-type
frame-relay inverse-arp
frame-relay lmi-n391dte
frame-relay lmi-n392dce
frame-relay lmi-n392dte
frame-relay lmi-n393dce
frame-relay lmi-n393dte
frame-relay lmi-t392dce
frame-relay lmi-type
frame-relay local-dlci
frame-relay map
frame-relay route
keepalive
show frame-relay lmi
show frame-relay map
show frame-relay pvc
show frame-relay traffic

debug frame-relay

Use this command to turn on the debug switch of the frame relay in privileged EXEC mode.
debug frame-relay {**events** | **lmi** | **packet**}

Parameter Description

Parameter	Description
events	Frame relay event
lmi	Local management information of frame relay
packet	Frame relay messages

Defaults No debug switch is turned on.

Command Mode Privileged EXEC mode

Configuration Examples The following example turns on the local management information debug switch of frame relay:

```
Ruijie# debug frame-relay lmi
```

Related Commands

Command	Description
undebug	Turns off the debug switch.

Platform Description N/A

Command History

Version	Description
N/A	N/A

clear frame-relay-inarp

Use this command to clear the dynamic address mapping created with the reverse ARP in privileged EXEC mode.

clear frame-relay-inarp

Parameter Description N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to clear all dynamic address mapping table so that the dynamic address mapping of frame relay is rebuilt. Executing this command may cause link interruption. So, when it is necessary to execute this command, ensure no loss of data in progress resulting from the link interruption.

Configuration Examples The following example clears the dynamic address list created with the reverse ARP:

```
Ruijie# clear frame-relay-inarp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description

N/A	N/A

encapsulation frame-relay

Use this command to encapsulate the frame relay protocol in interface configuration mode.
Use the **no** form of this command to restore the default installation of the interface.
encapsulation frame-relay [**ietf**]
no encapsulation frame-relay

Parameter Description

Parameter	Description
ietf	Standard RFC1490 encapsulation

Defaults CISCO encapsulation without ietf option.

Command Mode Interface configuration mode

Usage Guide For the compatibility with mainstream devices, the RGOS system takes the default frame relay encapsulation format of the CISCO encapsulation. If there is no special application, select the **ietf** type encapsulation generally, i.e. the **ietf** option of the command.
The CISCO encapsulation differs from the **ietf** encapsulation as follows: the CISCO encapsulation uses a 4-byte header (two bytes for DLCI, and the other two for the type of message).

Configuration Examples The following example specifies the ietf encapsulation type (standard encapsulation):

```
Ruijie(config-if)# encapsulation frame-relay ietf
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay interface-dlci

Use this command to specify the DLCI number for sub-interface in interface configuration mode.
Use the **no** form of this command to cancel the specified DLCI number.
frame-relay interface-dlci *dlci*
no frame-relay interface-dlci *dlci*

Parameter Description

Parameter	Description
dlci	DLCI number, ranging from 16 to 1007

Defaults No DLCI number specified

Command Mode Interface configuration mode

Usage Guide By default, when no DLCI is allocated for the sub-interface, all usable DLCIs belong to the master interface. Therefore, it is required to use this command to specify the DLCI number for the sub-interface.
This command is generally used in sub-interface. If the master interface runs a routing protocol that needs the reverse ARP, this command can also be used.
This command is required for all point-to-point interface and multipoint sub-interface that have the reverse ARP capability. It is not required for the multipoint sub-interface that uses static mapping.

Configuration Examples The following example specifies the DLCI number on the point-to-point sub-interface:

```
Ruijie(config)# interface serial 1/1.1 point-to-point
Ruijie(config-subif)# frame-relay interface-dlci 30
```

The following example specifies the DLCI number on the master interface:

```
Ruijie(config)# int serial 1/1
Ruijie(config-if)# frame-relay interface-dlci 30
```

Related Commands

Command	Description
show frame-relay pvc	Displays the PVC statistics on the interface.
show interface	Displays the interface statistic information.

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay intf-type

Use this command to specify the frame relay exchange type on the interface.
Use the **no** form of this command to restore the default exchange type.
frame-relay intf-type {**dce** | **dte** }
no frame-relay intf-type {**dce** | **dte** }

Parameter Description

Parameter	Description
dce	The router is emulated as the frame relay switch.
dte	The router is the data terminal device that connects the frame relay network.

Defaults **dte**

Command Mode Interface configuration mode

Usage Guide Before using this command, be sure to run the frame-relay switching command in global configuration mode to enable the frame relay exchange function.

Configuration Examples The following example specifies the frame relay type dce on the specified interface:

```
Ruijie(config)# frame-relay switching
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# frame-relay intf-type dce
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay inverse-arp

Use this command to enable the reverse ARP on the specified master interface or sub-interface.
Use the **no** form of this command to disable the reverse ARP on the interface.
frame-relay inverse-arp [**protocol**] [*dlci*]
no frame-relay inverse-arp [**protocol**] [*dlci*]

Parameter Description

Parameter	Description
protocol	Protocol type; only IP supported now
dlci	DLCI number, ranging from 16 to 1007

Defaults Reverse ARP enabled on the interface

Command Mode Interface configuration mode

Usage Guide The reverse ARP is implemented according to the RFC1293. It is used to find the opposite protocol (IP) address in case of the encapsulation of frame relay.
If the reverse ARP is disabled on the interface, using this command without any option enables the reverse ARP for all DLCI numbers, or using this command with the protocol and the DLCI number options enables the reverse ARP of the specified DLCI.
The reverse ARP and the static mapping are mutually exclusive. That, if the static mapping is specified for the DLCI number, the reverse ARP will not operate any more. The reverse ARP can be overwritten by the static mapping, and the inverse is impossible.

Configuration Examples The following example disables the reverse ARP:

```
Ruijie(config-if)# no frame-relay inverse-arp
```

Related Commands

Command	Description
clear frame-relay-inarp	Clears the mapping learned through reverse ARP.
show frame-relay map	Displays the frame relay mapping information.

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay lmi-n391dte

Use this command to set the PVC status polling interval.
Use the **no** form of this command to restore the default setting.
frame-relay lmi-n391dte *keep-exchanges*
no frame-relay lmi-n391dte

Parameter Description

Parameter	Description
keep-exchanges	Interval times, ranging from 1 to 255

Defaults 6

Command Mode Interface configuration mode

Usage Guide For the interface encapsulation DTE, the interface sends the status request messages to the frame relay switch at a fixed interval. There are two kinds of request messages: one is to ask the integrity of the link; the other is to ask the integrity of the link and ask the status of all PVCs, called the full status request message. The full status request message is sent once every **lmi-n391dte**. The other request messages ask only the link integrity.

For example, the full status request message is sent every 6 times by default, which means that the first to the fifth request messages are to ask the link integrity, while the sixth request message is the full status request message, and so on.

Configuration Examples The following example specifies the PVC status polling interval times as 5:

```
Ruijie(config-if)# frame-relay lmi-n391dte 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay lmi-n392dce

Use this command to set the threshold of the DCE interface error times.

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

frame-relay lmi-n392dce *threshold*

no frame-relay lmi-n392dce

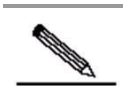
Parameter Description

Parameter	Description
threshold	Threshold of the error times, ranging from 1 to 10

Defaults 2

Command Mode Interface configuration mode

Usage Guide Among the N393 monitored events, when there are N392 continuous frame relay link errors, the link is advertised to be disconnected.



Note The value of the N393DCE must be greater than that of the N392DCE.

Configuration Examples The following example specifies the DCE error threshold as 4:

```
Ruijie(config-if)# frame-relay intf-type dce
Ruijie(config-if)# frame-relay lmi-n392dce 5
```

Related Commands

Command	Description
frame-relay lmi-n393dce	Specifyies the total number of DCE monitored events.

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay lmi-n392dte

Use this command to set the threshold of the DTE interface error times in interface configuration mode.

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

frame-relay lmi-n392dte *threshold*

no frame-relay lmi-n392dte

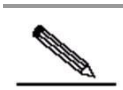
Parameter Description

Parameter	Description
threshold	Threshold of the error times, anging from 1 to 10

Defaults 3

Command Mode Interface configuration mode

Usage Guide Among the N393 monitored events, when there are N392 continuous frame relay link errors, the link is advertised to be disconnected.


Note The value of the N393DTE must be greater than that of the N392DTE.

Configuration Examples The following example specifies the DTE error threshold as 4:

```
Ruijie(config-if)# frame-relay intf-type dte
Ruijie(config-if)# frame-relay lmi-n392dte 4
```

Related Commands

Command	Description
frame-relay lmi-n393dte	Specifies the total number of DTE monitored events

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay lmi-n393dce

Use this command to set the total number of the DCE monitored events.

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

frame-relay lmi-n393dce *events*

no frame-relay lmi-n393dce

Parameter Description

Parameter	Description
events	Total number of monitored events, anging from 1 to 10

Defaults 2

Command Mode Interface configuration mode

Usage Guide The total number of monitored events is also called the LMI event counter. This parameter and the N392 define the conditions to advertise the RGOS link disconnection. In the N393 event, if the number of errors reaches N392, the RGOS advertise the link disconnection.

Note The value of the N393DCE must be greater than that of the N392DCE.

Configuration Examples The following example specifies the LMI event counter as 3:

```
Ruijie(config-if)# frame-relay intf-type dce
Ruijie(config-if)# frame-relay lmi-n393dce 3
```

Related Commands

Command	Description
frame-relay lmi-n392dce	Sets the DCE error threshold.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

frame-relay lmi-n393dte

Use this command to set the total number of the DTE monitored events.

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

frame-relay lmi-n393dte *events*

no frame-relay lmi-n393dte

Parameter Description	Parameter	Description
	events	Total number of monitored events, anging from1 to 10.

Defaults 4

Command Mode Interface configuration mode

Usage Guide The total number of monitored events is also called the LMI event counter. This parameter and the N392 define the conditions to advertise the RGOS link disconnection. In the N393 event, if the number of errors reaches N392, the RGOS advertise the link disconnection.

Note The value of the N393DTE must be greater than that of the N392DTE.

Configuration Examples The following example specifies the LMI event counter as 3:

```
Ruijie(config-if)# frame-relay lmi-n393dce 3
```

Related Commands	Command	Description
	frame-relay lmi-n392dte	Sets the DTE error threshold.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

frame-relay lmi-t392dce

Use this command to set the DCE polling timer time.
Use the **no** form of this command to restore the default setting.
frame-relay lmi-t392dce *seconds*
no frame-relay lmi-t392dce

Parameter Description

Parameter	Description
seconds	Timer time (in seconds), anging from 5 to 30

Defaults 15 seconds

Command Mode Interface configuration mode

Usage Guide When the DCE responds to the DTE request messages, if the DTE request message is not received within the period, the number of errors is added by 1.
The value of the T392 timer must be greater than the DTE Keepalive value.

Configuration Examples The following example specifies the T392 timer time as 20 seconds:

```
Ruijie(config-if)# frame-relay lmi-t392dce 20
```

Related Commands

Command	Description
keepalive(LMI)	Sets the keepalive timer of the LMI.

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay lmi-type

Use this command to set the type of the local management interface (LMI).
frame-relay lmi-type {**ansi** | **cisco** | **q933a**}

Parameter Description

Parameter	Description
ansi	Standard of the American National Standards Institute
cisco	CISCO type
q933a	CCITT type

Defaults **q933a**

Command Mode Interface configuration mode

Usage Guide The RGOS supports three LMI types: ANSI, CISCO and Q933A. The customer can select the appropriate LMI type according to the actual networking conditions.


Caution

The LMI type at both ends of the frame relay must be the same; otherwise the link cannot be up. Run the privileged mode command **show interface** to view the LMI type of the specified interface.

Configuration Examples The following example specifies the LMI type as ANSI:

```
Ruijie(config-if)# frame-relay lmi-type ansi
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay local-dlci

Use this command to specify the local source DLCI number of frame relay.

Use the **no** form of this command to cancel the specified source DLCI number.

frame-relay local-dlci *number*

no frame-relay local-dlci

Parameter Description

Parameter	Description
number	Source DLCI number, ranging 16 – 1007

Defaults No source DLCI number is specified.

Command Mode Interface configuration mode

Usage Guide This command is generally used in the case where the frame relay acts as the DCE encapsulation type, and is not used in the actual network environment. In the back-to-back environment, this local router is emulated as the DCE, and this command is used to provide the DLCI for the opposite DTE. One DCE interface supports only one DLCI number.

Configuration Examples The following example specifies the source DLCI number as 20:

```
Ruijie(config-if)# frame-relay local-dlci 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay map

Use this command to configure the frame relay static mapping.
Use the **no** form of this command to cancel the static mapping.
frame-relay map ip *address* **dlci** [**broadcast**] [**ietf** | **cisco**]
no frame-relay map ip *address*

Parameter Description

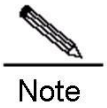
Parameter	Description
address	Opposite IP address
dlci	DLCI number for connecting the specified IP address
broadcast	Sends broadcast information at the specified IP address.
ietf	ietf frame relay encapsulation
cisco	cisco frame relay encapsulation

Defaults Static mapping is not specified.

Command Mode Interface configuration mode

Usage Guide The frame relay network supports the point-to-multipoint network. One physical interface supports multiple PVC connections. The static encryption mapping binds the remote address and the local DLCI in one-to-one manner.
The options **ietf** and **cisco** specifies the frame relay encapsulation type. If no option is used, the attribute of the **encapsulation frame-relay** is inherited. When a physical interface communicates

with multiple remote branches via multiple DLCIs, if some remote branches have different frame relay encapsulations, this option can be used to match the encapsulation types.



Note

In the static mapping, the encapsulation type has a higher priority than the **encapsulation frame-relay**. If the encapsulation type is specified in the static mapping, it overwrites the encapsulation type in the **encapsulation frame-relay** on the specified DLCI link.

If you want to run the routing protocol on the specified link, use the **broadcast** option.

Configuration Examples The following example specifies the remote address 30.1.1.1 mapping DLCI 30:

```
Ruijie(config-if)# frame-relay map ip 30.1.1.1 30 broadcast
```

Related Commands

Command	Description
encapsulation frame-relay	Encapsulates frame relay.

Platform Description N/A

Command History

Version	Description
N/A	N/A

frame-relay route

Use this command to specify the PVC switching static routes of frame relay.

Use the **no** form of this command to delete the specified PVC switching static route.

frame-relay route in-dlci interface serial *number* **out-dlci**

no frame-relay route in-dlci

Parameter Description

Parameter	Description
in-dlci	Local DCLI, for receiving data
number	Destination interface for forwarding data
out-dlci	Remote DLCI connected with the destination interface

Defaults PVC switching static mapping is not specified.

Command Mode Interface configuration mode

Usage Guide This command is mostly used to emulate the router as a frame relay switch in the lab environment. This command can be configured only at the DCE end. It is used for data forwarding between different interfaces to implement the capability to emulate frame relay switch.
The in-dlci option specifies the emulative DLCI that the current interface provides for the connected device (router). The *number* and out-dlci options specify the switched interface of the device and the DLCI number for establishing the PVC mapping.

Configuration Examples The following example specifies a static mapping on the synchronous interface 0/0, local DLCI as 100, switched interface of the device as synchronous interface 1, and switched interface mapping to the PVC 100-200:

```
Ruijie(config)# interface serial 0/0
Ruijie(config-if)# frame-relay route 100 interface serial 1 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

keepalive

Use this command to specify the keepalive time of the LMI.
Use the **no** form of this command to forbid the keepalive message.
keepalive *number*
no keepalive

Parameter Description

Parameter	Description
number	keepalive time, in seconds

Defaults 10 seconds

Command Mode Interface configuration mode

Usage Guide This command specifies the time interval for the router to send request messages to the frame relay switch. This interval must be less than the one defined with **frame-relay lmi-t392dce** in the switch.

Configuration Examples The following example specifies the keepalive period as 5 seconds:

```
Ruijie(config-if)# keepalive 5
```

Related Commands

Command	Description
Frame-relay lmi-t392dce	Sets the polling timer time of the DCE interface.

Platform Description N/A

Command History

Version	Description
N/A	N/A

show frame-relay lmi

Use this command to view the LMI statistics in privileged EXEC mode.

show frame-relay lmi [**interface serial** *number*]

Parameter Description

Parameter	Description
number	Interface number

Command Mode Privileged EXEC mode

Configuration Examples The following example shows the LMI statistical information:

```
Ruijie# sh frame-relay lmi
LMI Statistics for interface serial (Frame Relay DTE) LMI TYPE = CCITT
Invalid Unnumbered info 0      Invalid Prot Disc 0
Invalid dummy Call Ref 0       Invalid Msg Type 0
Invalid Status Message 0       Invalid Lock Shift 0
Invalid Information ID 0       Invalid Report ELE Len 0
Invalid Report Request 0       Invalid Keepalive ELE Len 0
Num Status Enq. Sent 806       Num Status msgs Rcvd 745
Num Update Status Rcvd 0       Num Status Timeouts 0
```

Parameter description:

The lines with the **invalid** option mean the received LMI message contain invalid number of messages of that kind of option.

Num status enq. Sent : Number of the sent LMI messages

Num status msgs Rsvd : Number of the received LMI messages

Num update status rcvd: Number of the received update LMI messages

Num status timeouts: Number of messages without receiving reply messages in time

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

show frame-relay map

Use this command to view the mapping of the current connection of the frame relay in privileged EXEC mode.

show frame-relay map

Parameter Description N/A

Command Mode Privileged EXEC mode

Configuration Examples The following example shows the output of the command:

```
Ruijie# sh frame-relay map
serial 1/0 (up): ip 1.1.1.1
dlci 100(0x1840), dynamic,
broadcast,CISCO, status: ACTIVE
```

Parameter description:

serial1/0(up): Interface status

ip 1.1.1.1: Destination address

dlci 100(0x1840): DLCI number, 100 for decimal denotation, 0x1840 for denotation in transmission lines

dynamic : Mapping type: static or dynamic

CISCO: Frame relay encapsulation type: IETF or CISCO

Active: Mapping status

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

show frame-relay pvc

Use this command to view the PVC statistics in privileged EXEC mode.

show frame-relay pvc [**interface** *interface*] [*dlci*]

Parameter Description

Parameter	Description
interface	Interface number.
dlci	DLCI number

Command Mode Privileged EXEC mode

Usage Guide This command with the *interface* option is used to view the PVC statistics of the specified interface, or it with the DLCI option to view the statistics of the specified DLCI. No option means displaying the statistics of all DLCIs on the current router.

Configuration Examples The following example shows the statistics of the specified DLCI (100):

```
Ruijie# show frame-relay pvc 30
PVC Statistics for interface serial 1/0 (Frame Relay DTE)
DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE , INTERFACE = serial 1/0
input pkts 100      output pkts 100     in bytes 2600
out bytes 3000      dropped pkts 0      in FECN pkts 0
in BECN pkts 0      out FECN pkts 0     out BECN pkts 0
in DE pkts 0        out DE pkts 0
The parameters can be visually understood.
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

show frame-relay traffic

Use this command to view the frame relay statistics since the last restart in privileged EXEC mode.

show frame-relay traffic

Parameter Description N/A

Command Mode Privileged EXEC mode

Configuration Examples The following example shows the output of the command:

```
Ruijie# show frame-relay traffic
Frame Relay Inverse Arp statistics:
Inarp requests sent 101, Inarp replies recvd 101
ARP request recvd 0, ARP replies sent 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

LAPB and X25 Configuration Command

Configuration Related Commands

The LAPB and X25 configuration involves the following related commands:

debug lapb
debug x25
encapsulation lapb
encapsulation x25
lapb k
lapb modulo
lapb n1
lapb n2
lapb t1
lapb t4
show x25 map
show x25 vc
x25 address
x25 hic
x25 hoc
x25 htc
x25 ips
x25 lic
x25 loc
x25 ltc
x25 map
x25 modulo
x25 ops
x25 pvc(encapsulation)
x25 t10
x25 t11
x25 t12
x25 t13
x25 t20
x25 t21
x25 t22
x25 t23
x25 win
x25 wout

debug lapb

Use this command to turn on the debug switch of the LAPB in privileged EXEC mode.

debug lapb

Parameter Description N/A

Command Mode Privileged EXEC mode

Configuration Examples The following example shows the output after the LAPB debug switch is turned on:

```
Ruijie# debug lapb
serial 1/3: LAPB I CONNECT (7) IFRAME 1 2
serial 1/3: LAPB O CONNECT (93) IFRAME 2 2
serial 1/3: LAPB I CONNECT (2) RR (R) 3
serial 1/3: LAPB I CONNECT (93) IFRAME 2 3
serial 1/3: LAPB O CONNECT (2) RR (R) 3
serial 1/3: LAPB O CONNECT (93) IFRAME 3 3
```

serial1/3: Name of the interface: O (output) for LAPB message output, I (input) for message input, SABMSENT for link status in the SAMB frame sending status, (2) for message length, SABM for frame type, P for Poll.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

debug x25

Use this command to turn on the debug switch of the X25 in privileged EXEC mode.

debug x25 [**events | packets**]

Parameter Description

Parameter	Description
events	Turns on the x25 negotiation event debug switch.
packets	Turns on the x25 message debug switch.

Command Mode Privileged EXEC mode

Configuration Examples The following example turns on the x25 debug switch:

```
Ruijie# debug x25 pa
X25 packet debugging is on
serial 1/3: X25 O P3 CALL REQUEST (13) 8 lci 1
From(4):2222 To(4):3333
Facilities: (0)
Call User Data (4): 0xcc0 0 0  (ip)!
serial 1/3: X25 I P3 CALL CONNECTED (5) 8 lci 1
From(0): To(0):
Facilities: (0)
serial 1/3: X25 O P4 DATA (91) 8 lci 1 PS 0 PR 0
serial 1/3: X25 I P4 DATA (91) 8 lci 1 PS 0 PR 1
serial 1/3: X25 O D1 DATA (91) 8 lci 1 PS 1 PR 1!
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

encapsulation lapb

Use this command to configure the encapsulation of LAPB.

encapsulation lapb [**dte** | **dce**]

Parameter Description

Parameter	Description
dte	Specifies the interface in the DTE working mode.
dce	Specifies the interface in the DCE working mode.

Defaults The default encapsulation for synchronous interfaces is HDLC.

No option with this command means the DTE working mode is enabled by default.

Command Mode Interface configuration mode

Usage Guide The LAPB is the layer-2 protocol of the X25. Generally the LAPB is used when the users connected with both ends are in full control. In case of the connection to the X25 network, only the X25 encapsulation can be used.

Configuration Examples The following example encapsulates the synchronous interface 1 as LAPB DCE:

```
Ruijie(config)# int serial 1
Ruijie(config-if)# encapsulation lapb dce
```

Related Commands

Command	Description
encapsulation x25	Encapsulates x25 protocol.

Platform Description N/A

Command History

Version	Description
N/A	N/A

encapsulation x25

Use this command to encapsulate the x25 protocol.
Use the **no** form of this command to restore the default encapsulation.
encapsulation x25 [**dte** | **dce**] [**ietf**]
no encapsulation x25 [**dte** | **dce**] [**ietf**]

Parameter Description

Parameter	Description
dte	Specifies the interface in the DTE working mode.
dce	Specifyies the interface in the DCE working mode.
ietf	Specifies the encapsulation type as the IETF standard encapsulation.

Defaults The default encapsulation for synchronous interfaces is HDLC.
The default X25 working mode is DTE, and the default encapsulation type is CISCO encapsulation.

Command Mode Interface configuration mode

Usage Guide An x25 connection requires DTE at one end and DCE at the other end. Generally the terminal on the user side acts as the DTE, and the terminal on the office side acts as the DCE.
For the computability with the routers of key manufacturers, the RGOS supports the CISCO type x25 encapsulation of the default encapsulation type. So in the actual configurations, it is necessary to confirm the x25 encapsulation type of the opposite end.

The X25 DTE/DCE working mode is the interface specifications between the office end and the user end, which is different from the router back-to-back connection with the V35DTE/DCE cable.

Configuration Examples The following example specifies synchronous interface as **ietf x25 dte**:

```
Ruijie(config-if)# encapsulation x25 dte ietf
```

Related Commands

Command	Description
X25 map	Specifies the x25 mapping.

Platform Description N/A

Command History

Version	Description
N/A	N/A

lapb k

Use this command to set the size of the LAPB slip window.
lapb k *window-size*

Parameter Description

Parameter	Description
window-size	Size of the slip window, ranging from 1 to LAPB modulo value minus 1. (if the modulo is 8, the value range is 1 - 7; if the modulo is 128, the value range is 1 - 127.)

Defaults 7 frames, default modulo 8

Command Mode Interface configuration mode

Usage Guide The slip window means the maximum number of frames whose data are not confirmed by the peer end, default value recommended. The size of the slip window must match the setting value for the packet switching network on the office side; otherwise it may cause continuous data retransmission. The value change of slip window does not take effect immediately until the LAPB is reset.

Configuration Examples The following example specifies the size of LAPB slip window as 15 frames:

```
Ruijie(config-if)# lapb modulo 128
Change held until LAPB is reset
Ruijie(config-if)# lapb k 15
Change held until LAPB is reset
```

Related Commands

Command	Description
lapb modulo	Sets LAPB modulo.

Platform Description N/A

Command History

Version	Description
N/A	N/A

lapb modulo

Use this command to set the LAPB modulo.

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

lapb modulo *modulo*

no lapb modulo

Parameter Description

Parameter	Description
modulo	modulo 8 or modulo 12

Defaults Modulo 8

Command Mode Interface configuration mode

Usage Guide The modulo of the LAPB protocol determines the value range of the slip window. The maximum of the LAPB slip window can only be equal to modulo-1. There are two numbering methods of LAPB frames: modulo 8 and modulo 128. Every data frame (I frames) are numbered sequentially, from 0 to modulo-1. The sequential number is recycled in the range of the modulo.
The local LAPB modulo must be consistent with the office end; otherwise it may lead to continuous data retransmission. The X25 modulo differs from the LAPB modulo but they are set by using the same command.
The value change of LAPB modulo does not take effect immediately until the LAPB is reset.

Configuration Examples The following example specifies the LAPB extension mode (modulo 128) for the router:

```
Ruijie(config-if)# lapb  modulo 128
Change held until LAPB is reset
```

Related Commands

Command	Description
lapb k	Sets the size of the LAPB slip window.

Platform Description N/A

Command History

Version	Description
N/A	N/A

lapb n1

Use this command to set the maximum length of the LAPB frame.
Use the **no** form of this command to restore the default setting.
lapb n1 *bits*
no lapb n1

Parameter Description

Parameter	Description
bits	Frame size, in unit of bit, valid only for multiples of 8. The value range changes with the MTU, which can be viewed by using the ? command.

Defaults Maximum of the current valid value

Command Mode Interface configuration mode

Usage Guide The N1 is the maximum length of the LAPB frame. The minimum is determined by the default message size, and the maximum is determined by the MTU.
Changing this parameter does not increase transmission efficiency at all. However, inconsistent parameter settings at both ends may cause link failure. So, it is not recommended to the change the default of the parameter.

Configuration Examples The following example specifies the maximum length of the LAPB frame as 12,000 bits:

```
Ruijie(config-if)# lapb n1 12000
```

Related Commands

Command	Description
mtu	Sets the MTU value.
show interface	Displays the interface information, including the LAPB parameters.

Platform Description N/A

Command History

Version	Description
N/A	N/A

lapb n2

Use this command to set the maximum transmission times (retransmission times) of the LAPB data frame.
Use the **no** form of this command to restore the default setting.
lapb n2 *tries*
no lapb n2

Parameter Description

Parameter	Description
tries	Retransmission times ranging from 1 to 255

Defaults 20

Command Mode Interface configuration mode

Usage Guide This parameter is the LAPB N2 parameter, the maximum times to resend the LAPB data. When exceeded, the LAPB link protocol turns from UP to Down.

Configuration Examples The following example specifies the maximum LAPB retransmitting times as 30:

```
Ruijie(config-if)# lapb n2 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

lapb t1

Use this command to set the LAPB data frame retransmission timeout time.
Use the **no** form of this command to restore the default setting.
lapb t1 *milliseconds*
no lapb t1

Parameter Description

Parameter	Description
milliseconds	Millisecond, ranging from 0 to 64,000

Defaults 3000ms

Command Mode Interface configuration mode

Usage Guide If the line is of poor quality and runs slowly, this command can be used to increase the message retransmission timeout time to prevent too many data retransmissions that result in line jam.
The timeout time can be adjusted by referring to the result of Ping destination address.

Configuration Examples The following example specifies the LAPB data timeout time as 4000ms:

```
Ruijie(config-if)# lapb t1 4000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description

N/A	N/A

lapb t4

Use this command to set the LAPB link detection time.
Use the **no** form of this command to restore the default setting.
lapb t4 *seconds*
no lapb t4

Parameter Description

Parameter	Description
seconds	Detection time, in seconds ranging from 0 to 255

Defaults 0 seconds

Command Mode Interface configuration mode

Usage Guide Once the LAPB receives a frame, it resets the link detection timer (T4). If T4 expires, the LAPB immediately sends an RR frame with the Poll tag. If no response to the RR frame is received, LAPB disconnects the link and initiates negotiation again.
The non-zero T4 value must be greater then the retransmitting timeout time (T1).

Configuration Examples The following example specifies the link detection time as 8 seconds:

```
Ruijie(config-if)# lapb t4 8
```

Related Commands

Command	Description
lapb t1	Sets the retransmission timeout time.
lapb n2	Sets the retransmission times.

Platform Description N/A

Command History

Version	Description
N/A	N/A

show x25 map

Use this command to show the x25 address mapping table.
show x25 map

Parameter Description N/A

Command Mode Privileged EXEC mode

Configuration Examples The following example shows an instance of the command:

```
Ruijie# sh x25 map
serial 1/3: X.121 3333 <--> ip 2.2.2.2
PERMANENT, 1 VC: 1
```

Serial 1: Interface mapping the encapsulation
x.121 3333: Opposite x.121 address
ip 2.2.2.2: Opposite IP address
permanent: x25 mapping type: permanent indicates the mapping is defined via x25; the PVC type indicates the mapping is defined via x25 pvc.
1 vc: Virtual circuit (SVC or PVC) corresponding to the mapping
1: Virtual circuit ID

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

show x25 vc

Use this command to view the X25 virtual circiut (SVC or PVC) information.
show x25 vc

Command Mode Privileged EXEC mode

Usage Guide The LCN option is used to view the information of the specified virtual circuit. The command without the LCN option shows the information of all virtual circuits.

Configuration Examples The following example shows an instance of the command.

```
Ruijie# show x25 vc
SVC 1, State: D1, Interface: serial 1/3
Connects 3333 <--> ip 2.2.2.2
```

```
no Tx data PID
Window size input: 2, output: 2
Packet size input: 128, output: 128
PS: 5  PR: 5  ACK: 4  Remote PR: 5  RCNT: 1  RNR: FALSE
Retransmits: 0  Reassembly (bytes): 0
Held Fragments/Packets: 0/0
Bytes 440/440 Packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Svc 1: The virtual circuit is the type of the switching virtual circuit, numbering 1024

State: D1 : Virtual circuit status; refer to the ITU-TX25 recommendations for its definition.

Interface :serial1: Interface where the virtual circuit is located

Connects 3333 <--> ip 2.2.2.2: x.121 address and IP address associated with the virtual circuit

Data pid: Method for identifying data in transmitting data, including none and ietf

Window size: Size of the slip window

Packet size: Maximum message size of the virtual circuit

PS: Current transmission sequential number

PR: Sequential number of the next packet expected

ACK: Last response message received; sequential number of the confirmed packet for the received message; used for window slip

Remote PR: Sequential number of the next packet expected by the opposite end

RCNT: Received message without response

RNR: Receiving not ready status; refuse the opposite end to send further data when the buffer is nearly full; functioning for flow control

Retransmits: Statistics of retransmissions

Timer (secs): Non-zero value indicates waiting for the response message from the opposite

Reassembly (bytes): Redistributed messages

Held Fragments/Packets: Fragment and messages to be combined for transmission

Bytes: Bytes of the transmitted and received data since the creation of the virtual circuit

Packets: Number of the transmitted and received packets since the creation of the virtual circuit

Resets: Number of the transmitted and received reset packets since the creation of the virtual circuit

RNRs: Number of the transmitted and received "data receiving not ready" packets since the creation of the virtual circuit

REJs: Number of the transmitted and received rejecting packets since the creation of the virtual circuit

INTs: Number of the transmitted and received interruption packets since the creation of the virtual circuit

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Command History

Version	Description

N/A	N/A

x25 address

Use this command to configure the x.121 address of the specified interface.
Use the **no** form of this command to delete the specified x.121 address.
x25 address *x121-address*
no x25 address

Parameter Description

Parameter	Description
x121-address	x.121 address, allocated by the X.25 packet switching center (office)

Defaults The x.121 address of the interface is not specified.

Command Mode Interface configuration mode

Usage Guide When a synchronous interface is connected with the public data network, this command is used to configure the x121 address allocated by the X.25 packet switching center.
If it is a private network, the x121 address can be configured randomly.
If the router acts as the x.25 switch, it is not required to configure the x.121 address.

Configuration Examples The following example specifies x121 address of synchronous interface 1 as 1111:

```
Ruijie(config)# interface serial 1
Ruijie(config-if)# x25 address 1111
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 hic

Use this command to set the highest unidirectional incoming logical channel of X.25.
x25 hic *circuit-number*

Parameter Description

Parameter	Description
circuit-number	Virtual circuit ID, ranging from 1 to 4095, 0 indicating no HIC range

Defaults 0

Command Mode Interface configuration mode

Usage Guide If it is not allowed to call out from the DTE end, set the bidirectional incoming/outgoing logical channel (LTC and HTC) as 0 and specify the incoming logical channel value at the same time. The incoming logical channel (LIC and HIC) must be smaller than the bidirectional incoming/outgoing logical channel (LTC and HTC); the bidirectional incoming/outgoing logical channel is smaller than the outgoing logical channel (LOC and HOC). The value of the HIC must be the same as the parameter provided by the office.
For more details of X.25 logical channel, see WAN Protocol Configuration Guide.

Configuration Examples The following example specifies the HIC as 10:

```
Ruijie(config-if)# x25 hic 10
Parameter change held until a RESTART event
```

Related Commands

Command	Description
x25 lic	Sets the minimum unidirectional incoming logical channel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 hoc

Use this command to set the highest unidirectional outgoing logical channel.
x25 hoc *circuit-number*

Parameter Description

Parameter	Description
circuit-number	Logical channel number, ranging from 1 to 4095, 0 indicating no HOC range

Defaults 0

Command Mode Interface configuration mode

Usage Guide If it is not allowed to receive calls at the DTE end, set the bidirectional incoming/outgoing logical channel (LTC and HTC) as 0 and specify the incoming logical channel value (HOC and LOC) at the same time. The outgoing logical channel (LOC and HOC) must be greater than the bidirectional incoming/outgoing logical channel. The value of the HOC must be the same as the parameter provided by the office.
For more details of X.25 logical channel, see WAN Protocol Configuration Guide.

Configuration Examples The following example specifies the outgoing logical channel as 1000 - 1100:

```
Ruijie(config-if)# x25 loc 1000
Parameter change held until a RESTART event
Ruijie(config-if)# x25 hoc 1100
Parameter change held until a RESTART event
```

Related Commands

Command	Description
X25 loc	Sets the minimum unidirectional outgoing logical channel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 htc

Use this command to set the highest bidirectional incoming/outgoing logical channel of X.25.
x25 htc *circuit-number*

Parameter Description

Parameter	Description
circuit-number	Logical channel number, ranging from 1 to 4095, 0 indicating no HTC range

Defaults 1024

Command Mode Interface configuration mode

Usage Guide The bidirectional incoming/outgoing logical channel (LTC and HTC) must be greater than the incoming logical channel (LIC and HIC), and smaller than the outgoing logical channel (LOC and HOC). The value of the HTC must be the same as the parameter provided by the office.
For more details of X25 logical channel, see the *WAN Protocol Configuration Guide*.

Configuration Examples The following example specifies the valid values for HTC and LTC:

```
Ruijie(config-if)# x25 htc 1000
Parameter change held until a RESTART event
Ruijie(config-if)# x25 ltc 900
Parameter change held until a RESTART event
```

Related Commands

Command	Description
X25 ltc	Sets the minimum bidirectional incoming/outgoing X.25 logical channel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 ips

Use this command to set the maximum size of the X.25 input message.
Use the **no** form of this command to restore the default setting.
x25 ips *size*
no x25 ips

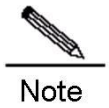
Parameter Description

Parameter	Description
size	Bytes (the value must be any of 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096)

Defaults 128 bytes

Command Mode Interface configuration mode

Usage Guide A message larger than the OPS will be divided into multiple fragment packets for transmission. Every fragment packet is tagged with M-bit, and they will be reassembled into a complete message at the receiving side. The network administrator can use this command to adjust the IPS value to reduce the message fragment/assembly according to the dataflow size in the network.



The input maximum message size (IPS) shall be the same as the output maximum message size (OPS). The value of the IPS must be the same as the parameter provided by the office.

Configuration Examples The following example specifies the IPS and OPS as 1024:

```
Ruijie(config-if)# x25 ips 1024
Parameter change held until a RESTART event
Ruijie(config-if)# x25 ops 1024
Parameter change held until a RESTART event
```

Related Commands

Command	Description
X25 ops	Sets the maximum size of output message.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 lic

Use this command to set the lowest unidirectional incoming logical channel of X.25.

x25 lic *circuit-number*

Parameter Description

Parameter	Description
circuit-number	Virtual circuit ID, ranging from 1 to 4095, 0 indicating no LIC range

Defaults 0

Command Mode Interface configuration mode

Usage Guide If it is not allowed to call out from the DTE end, set the bidirectional call-in/out logical channel (LTC and HTC) as 0 and specify the incoming logical channel value at the same time. The incoming logical channel (LIC and HIC) must be smaller than the bidirectional incoming/outgoing logical channel (LTC and HTC); the bidirectional incoming/outgoing logical channel is smaller than the outgoing logical channel (LOC and HOC). The value of the LIC must be the same as the parameter provided by the office.

For more details of X.25 logical channel, see WAN Protocol Configuration Guide.

Configuration Examples The following example specifies the HIC as 10:

```
Ruijie(config-if)# x25 lic 10
Parameter change held until a RESTART event
```

Related Commands

Command	Description
x25 hic	Sets the maximum unidirectional incoming logical channel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 loc

Use this command to set the lowest unidirectional outgoing logical channel.

x25 loc *circuit-number*

Parameter Description

Parameter	Description
circuit-number	Logical channel number, ranging from 1 to 4095, 0 indicating no LOC range

Defaults 0

Command Mode Interface configuration mode

Usage Guide If it is not allowed to receive calls at the DTE end, set the bidirectional incoming/outgoing logical channel (LTC and HTC) as 0 and specify the incoming logical channel value (HOC and LOC) at the same time. The outgoing logical channel (LOC and HOC) must be greater than the bidirectional incoming/outgoing logical channel. The value of the LOC must be the same as the parameter provided by the office.

For more details of X.25 logical channel, see WAN Protocol Configuration Guide.

Configuration Examples The following example specifies the outgoing logical channel as 1000 - 1100:

```
Ruijie(config-if)# x25 loc 1000
Parameter change held until a RESTART event
Ruijie(config-if)# x25 hoc 1100
Parameter change held until a RESTART event
```

Related Commands

Command	Description
X25 hoc	Sets the highest unidirectional outgoing logical channel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 ltc

Use this command to set the lowest bidirectional incoming/outgoing logical channel of X.25.

x25 ltc *circuit-number*

Parameter Description

Parameter	Description
circuit-number	Logical channel number, ranging from 1 to 4095, 0 indicating no LTC range

Defaults 1024

Command Mode Interface configuration mode

Usage Guide The bidirectional incoming/outgoing logical channel (LTC and HTC) must be greater than the incoming logical channel (LIC and HIC), and smaller than the outgoing logical channel (LOC and HOC). The value of the LTC must be the same as the parameter provided by the office.

For more details of X.25 logical channel, see the *WAN Protocol Configuration Guide*.

Configuration Examples The following example specifies the valid values for HTC and ITC:

```
Ruijie(config-if)# x25 htc 1000
Parameter change held until a RESTART event
Ruijie(config-if)# x25 ltc 900
Parameter change held until a RESTART event
```

Related Commands

Command	Description
X25 htc	Set the highest bidirectional incoming/outgoing X.25 logical channel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 map

Use this command to specify the mapping between X121 addresses and IP addresses.
Use the **no** form of this command to cancel the mapping between X121 addresses and IP addresses.
x25 map ip *address x121-address* [**option**]
no x25 map ip *address x121-address*

Parameter Description

Parameter	Description
address	Remote IP address
x121-address	Remote x121 address
option	Parameter option; see the guide for details.

Defaults No mapping is specified between X121 addresses and IP addresses.

Command Mode Interface configuration mode

Usage Guide This command can have different options to configure the user facility parameter (same as the X25 Facility), encapsulation method (including CISCO/IEFT), broadcast option and more mapping options .
If you want to run the OSPF or another routing protocol in the X25 network, use the **broadcast** option.
To modify the configured X25 mapping, it is only possible to delete the specified x25 mapping and then configure it again.
The mapping parameter options are explained as follows;
broadcast: Broadcast option; allow run the routing protocol on the specified x121 address
no-**incoming**: The mapping only used for initiating calls
no-**outgoing**: The mapping only used for accepting calls

Configuration Examples The following example maps the remote IP address 40.1.1.1 and X121 address 1111, and use the broadcast option at the same time:

```
Ruijie(config-if)# x25 map ip 40.1.1.1 1111 broadcast
```

Related Commands

Command	Description
ip ospf network	Specifies the OSPF network type.
show x25 map	Displays the X25 mapping type.
x25 facility	Sets the X25 user facility.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 modulo

Use this command to set the x25 modulo.

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

x25 modulo *modulo*

no x25 modulo

Parameter Description

Parameter	Description
modulo	Modulo value: 8 or 128.

Defaults 8

Command Mode Interface configuration mode

Usage Guide The x25 modulo value determines the size of the x25 slip window.

The X25 modulo value must match the parameters provided by the packet switching center of the office end.

Configuration Examples The following example specifies the x25 modulo as 128:

```
Ruijie(config-if)# x25 modulo 128
```

Related Commands

Command	Description
x25 facility	Defines the X.25 user facility parameter.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 ops

Use this command to set the maximum size of the X.25 output message.
Use the **no** form of this command to restore the default setting.
x25 ops *size*
no x25 ops

Parameter Description

Parameter	Description
size	Bytes (the value must be any of 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096)

Defaults 128 bytes

Command Mode Interface configuration mode

Usage Guide A message larger than the OPS will be divided into multiple fragment packets for transmission. Every fragment packet is tagged with M-bit, and they will be reassembled into a complete message at the receiving side. The network administrator can use this command to adjust the OPS value to reduce the message fragment/assembly according to the data flow size in the network.


Note

The input maximum message size (IPS) shall be the same as the output maximum message size (OPS).

Configuration Examples The following example specifies the IPS and OPS as 1024:

```
Ruijie(config-if)# x25 ips 1024
Parameter change held until a RESTART event
Ruijie(config-if)# x25 ops 1024
Parameter change held until a RESTART event
```

Related Commands

Command	Description
X25 ips	Sets the maximum size of input message.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 pvc (encapsulation)

Use this command to create the mapping from PVC to IP addresses.
Use the **no** form of this command to cancel the specified PVC mapping.
x25 pvc circuit ip *address x121-address* [**option**]
no x25 pvc *circuit*

Parameter Description

Parameter	Description
circuit	Virtual circuit channel number, which must be less than the number of the lowest unidirectional incoming logical channel LIC of the switching virtual circuit
address	Opposite IP address
x121-address	Opposite x121 address
option	Parameter option; see the guide for details.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command specifies the mapping between PVC and IP addresses, and then it is not required to configure the x25 mapping with the **x25 map** command. This command includes an x25 mapping.
The parameter options are described as follows:
broadcast : Broadcast option; allow run the routing protocol on the specified x121 address

Configuration Examples The following example specifies a PVC mapping:

```
Ruijie(config-if)# x25 pvc 12 ip 40.1.1.1 1111 broadcast
```

Related Commands

Command	Description
X25 map	Defines the x25 mapping.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t10

Use this command to set the timeout time (T10) of the X.25 DCE restart request.
Use the **no** form of this command to restore the default setting.
x25 t10 *seconds*
no x25 t10

Parameter Description

Parameter	Description
seconds	Timeout period, in seconds

Defaults 60 seconds

Command Mode Interface configuration mode

Configuration Examples The following example specifies the T10 timeout period as 40 seconds:

```
Ruijie(config-if)# x25 t10 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t11

Use this command to set the accepting call request timeout time (T101) of the X.25 DCE incoming request.
Use the **no** form of this command to restore the default setting.
x25 t11 *seconds*
no x25 t11

Parameter Description

Parameter	Description

seconds	Timeout period, in seconds

Defaults 180 seconds

Command Mode Interface configuration mode

Configuration Examples The following example specifies the T11 timeout period as 140 seconds:

```
Ruijie(config-if)# x25 t11 140
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t12

Use this command to set the indication timeout time (T12) of the X.25 DCE reset**.**

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

x25 t12 *seconds*

no x25 t12

Parameter Description

Parameter	Description
seconds	Timeout period, in seconds

Defaults 60 seconds

Command Mode Interface configuration mode

Configuration Examples The following example specifies the T12 timeout period as 30 seconds:

```
Ruijie(config-if)# x25 t12 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t13

Use this command to set the indication timeout time (T13) of the X.25 DCE release**.**

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

x25 t13 *seconds*

no x25 t13

Parameter Description

Parameter	Description
seconds	Timeout period, in seconds

Defaults 60 seconds

Command Mode Interface configuration mode

Configuration Examples The following example specifies the timeout period as 30 seconds:

```
Ruijie(config-if)# x25 t13 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t20

Use this command to set the timeout time (T20) of the X.25 DTE restart request.

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

x25 t20 *seconds*

no x25 t20 *seconds*

Parameter Description

Parameter	Description
seconds	Timeout period, in seconds

Defaults 180 seconds

Command Mode Interface configuration mode

Configuration Examples The following example specifies the T20 timeout period as 40 seconds:

```
Ruijie(config-if)# x25 t20 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t21

Use this command to set the timeout time (T21) of the X.25 DTE call request**.**

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

x25 t21 *seconds*

no x25 t21 *seconds*

Parameter Description

Parameter	Description
seconds	Timeout period, in seconds

Defaults 200s

Command Mode Interface configuration mode

Configuration Examples The following example specifies the timeout period as 140 seconds:

```
Ruijie(config-if)# x25 t21 140
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t22

Use this command to set the timeout time (T22) of the X.25 DTE reset request**.**

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

x25 t22 *seconds*

no x25 t22 *seconds*

Parameter Description

Parameter	Description
seconds	Timeout period, in seconds

Defaults 180 seconds

Command Mode Interface configuration mode

Configuration Examples The following example specifies the timeout period as 90 seconds:

```
Ruijie(config-if)# x25 t22 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 t23

Use this command to set the indication timeout time (T23) of the X.25 DTE release**.**

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

x25 t23 *seconds*

no x25 t23 *seconds*

Parameter Description

Parameter	Description
seconds	Timeout period, in seconds

Defaults 180 seconds

Command Mode Interface configuration mode

Configuration Examples The following example specifies the timeout period as 30 seconds:

```
Ruijie(config-if)# x25 t23 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 win

Use this command to set the size of the input slip window.

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

x25 win *packets*

no x25 win

Parameter Description

Parameter	Description
packets	Size of the slip window, ranging from 1 to x25 modulo minus 1.

Defaults 2 messages

Command Mode Interface configuration mode

Usage Guide This command determines the default number of messages for the router to send response, which can be overwritten by **x25** th.

To improve the bandwidth utilization of the line, this command can be used to set the slip window value as a value as big as possible.

The input/output slip window values configured with **x25** win and **x25 wout** must be the same unless the network supports asymmetrical input/output slip window size.

Configuration Examples The following example specifies the size of input window as 5 messages:

```
Ruijie(config-if)# x25 win 5
```

Related Commands

Command	Description
x25 wout	Sets x25 output slip window value.
X25 th	Sets the maximum for sending data message responses.
X25 modulo	Sets the x25 modulo.

Platform Description N/A

Command History

Version	Description
N/A	N/A

x25 wout

Use this command to set the size of the output slip window.

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

x25 wout *packets*

no x25 wout

Parameter Description

Parameter	Description
packets	Size of the slip window, ranging from 1 to x25 modulo minus 1.

Defaults 2 messages

Command Mode Interface configuration mode

Usage Guide This command determines the default number of message that can be sent before the router receives the response. To improve the bandwidth utilization of the line, this command can be used to set the slip window value as a value as big as possible.

The input/output slip window values configured with x25 win and **x25 wout** must be the same unless the network supports asymmetrical input/output slip window size.

Configuration Examples The following example specifies the size of output window as 5 messages:

```
Ruijie(config-if)# x25 wout 5
```

Related Commands

Command	Description
x25 win	Sets x25 output slip window value.
X25 th	Sets the maximum for sending data message responses.
X25 modulo	Sets the x25 modulo.

Platform Description N/A

Command History

Version	Description
N/A	N/A

DLDP Commands

dldp ip

Use this command to enable the DLDP detection function.

Use the **no** form of this command to disable the DLDP detection function for the specified IP address.

dldp ***ip*** **[*nexthopip*] [**interval ***value*** | retry ***value*** | resume **value]**

no dldp ***ip*** **[*nexthopip*]**

Parameter Description

Parameter	Description
ip	Peer IP address
nexthopip	Nexthop IP address
interval	Detection interval time. The valid range is 1-3600, in tick. (1 tick roughly equals 10ms)
retry	Retransmission times. The valid range is 1-3600.
resume	Resume times of the link of the peer device detected. Before the link state changes from DOWN to UP, the continuous DLDP detection packets shall be received. The valid range is 1-200.

Defaults

Interval:100ms;
Retry:3;
Working mode: passive mode;
Resume: 1.

Command Mode

Interface configuration mode

Usage Guide

Use this command to enable the DLDP detection function for the rapid detection of the Ethernet link error.

Configuration Examples

Example 1: The following example shows how to enable the DLDP function for the device 10.83.132.10:

```
Ruijie(config)# interface fastethernet 1/0
Ruijie(config-if)# dldp 10.83.132.1
Ruijie(config-if)#
```

Example 2: The following example shows how to enable the DLDP function in the passive mode:

```
Ruijie(config-if)# dldp passive.
```

Example 3: The following example shows how to enable the DLDP function for the across-network-segment device 20.1.1.1 with the nexthop ip 10.1.1.1:

```
Ruijie(config)# dldp 20.1.1.1 10.1.1.1
```

Example 4: The following example shows how to set the resume as 3:

```
Ruijie(config)# dldp 1.1.1.1 resume 3
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

Version Description N/A

Command History	Version	Description
	N/A	N/A

show dldp

Use this command to show the UP and DOWN times on the Ethernet interface in a period time.

show dldp interface [] [fastEthernet/GigabitEthernet *interface-number*]

Parameter Description	Parameter	Description
	interface-number	Specifies the Ethernet interface number to the dldp status of next interface only.
	Enter	Press the Enter to show the dldp status on all interfaces.

Command Mode Privileged EXEC mode

Usage Guide Use this command to show the UP and DOWN times in a period time on one/all Ethernet interfaces.
Dldp: the dldp link configured.
Down times: times of the dldp link chaning from UP to DOWN since last reset.
Up times: times of the dldp link changing from DOWN to UP since last reset.
Start times: the last reset system time

Configuration Examples **Example 1:** The following example shows the dldp state of the Ethernet interface 0/1:

```
Ruijie(config)#show dldp fastEthernet 0/0.1
```

```
================= FastEthernet 0/0.1 ==================
dldp      down times  up times start time
dldp 8.8.8.1   1      2    1970-0-1 0:0:31
dldp 8.8.8.10   1      2    1970-0-1 0:0:31
dldp 8.8.8.9   1      2    1970-0-1 0:0:31
```

Example 2: The following example shows the dldp state of all Ethernet interfaces :

```
 Ruijie(config)#show dldp interface
Ruijie#sh dldp interface
 ==================FastEthernet 0/0 ====================
dldp      down times  up times start time
dldp 7.7.7.1   3       4    2009-1-1 0:0:31
==================FastEthernet0/0.1 ==================
dldp       down times  up times start time
dldp 8.8.8.1    1       1    2009-1-1 0:0:31
dldp 8.8.8.10   1       1    2009-1-1 0:0:31
dldp 8.8.8.9    1       1    2009-1-1 0:0:31
==================FastEthernet 0/1 ====================
dldp       down times  up times start time
dldp 9.7.7.1    3       2    2009-1-1 0:0:31
```

clear dldp

Use this command to clear the UP and DOWN times recorded by the link DLDP enabled and then recalculate the times.

clear-dldp[all][destip[*nexthopip*]]

Parameter Description

Parameter	Description
destip	Destination IP address for the DLDP detection, which is used to clear the UP and DOWN times recorded in the link with IP address specified.
all	Clears all UP and DOWN times recorded of all Ethernet interfaces.
nexthopip	Clears the UP and DOWN times recorded if the nexthop exists.

Command Mode

Privileged EXEC mode

Usage Guide

The dldp records the number of UP and DOWN. With this command executed, the UP and DOWN times recorded in the specified/all link on the Ethernet interface are cleared and reset to 0.

Configuration Examples

Example 1: The following example shows how to clear the up/down statistical times of all dldps on the Ethernet interface 0/0:

```
Ruijie(config)#interface fastEthernet 0/0
Ruijie(config-if-FastEthernet 0/0)#clear-dldp all
```

Example 2: The following example shows how to clear the up/down statistical times of the dldp 1.1.1.1 on Ethernet interface 0/0:

```
Ruijie(config)#interface fastEthernet 0/0
Ruijie(config-if-FastEthernet 0/0)#clear-dldp 1.1.1.1
```

Example 3: The following example shows how to clear the up/down statistical times of the dldp 20.1.1.1 10.1.1.1 on Ethernet interface 0/0:

```
Ruijie(config)#interface fastEthernet 0/0
Ruijie(config-if-FastEthernet 0/0)#clear-dldp 20.1.1.1 10.1.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Command History

Version	Description
N/A	N/A

BFD Configuration Commands

bfd

Use this command to set the BFD session parameters in 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 *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

Parameter Description

Parameter	Description
interval *milliseconds*	Interval of sending the BFD control messages to the BFD session neighbor. *milliseconds:* valid range from 50ms to 10000ms.
min_rx *milliseconds*	Expected interval of receiving the BFD control messages from the BFD session neighbor. *milliseconds:* valid range from 50ms to 10000ms.
multiplier *multiplier-value*	Count of BFD control messages not received from the peer in the configured interval. *multiplier-value:* valid range from 3 to 50.

Defaults No BFD session parameters are configured by default. Those parameters must be configured before you enable 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 you enable BFD on the routers.

Configuration Examples The following example shows how to configure the BFD session parameters on Routed Port FastEthernet 0/2:

```
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config)# no switchport (this command is not available for routers)
Ruijie(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

Related Commands

Command	Description
bfd all-interfaces	Configures BFD for all route protocols on the interface.
clear bfd	Clears the BFD session statistics.
ip ospf bfd	Configures BFD for OSPF.
ip rip bfd	Configures BFD for RIP.

Platform N/A

Description

Command History	Version	Description
	10.3(4b3)	New command
	10.3(5)	Modified the parameter range of the BFD session.

bfd all-interfaces

Use this command to configure the BFD for the route protocols in (RIP, OSPF) router configuration mode.
Use the **no** form of this command to disable this function.
bfd all-interfaces
no bfd all-interfaces

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, BFD cannot be configured for all route protocols on the interface.

Command Mode Route configuration mode

Usage Guide Use the following two methods to enable or disable the BFD configuration for route protocols on the interface:
Use the **[no] bfd all-interfaces** command in the OSPF and RIP route configuration mode;
Use the **ip ospf bfd** [**disable**] or **ip rip bfd** [**disable**] command in the interface configuration mode.

Configuration Examples The following example shows how to configure the BFD for OSPF on alll interfaces:

```
Ruijie(config)# router ospf 123
Ruijie(config-router)# bfd all-interface
```

Related Commands	Command	Description
	bfd	Configures the BFD session parameters.
	ip ospf bfd	Configures the BFD for OSPF.
	ip rip bfd	Configures the BFD for RIP.

Platform Description N/A

Command History	Version	Description
	10.3(4b3)	New command

bfd cpp

Use this command to enable the BFD protection policy in global configuration mode.
Use the **no** form of this command to disable BFD CPP.
bfd cpp
no bfd cpp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The BFD protection policy 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 shows how to enable the BFD protection policy:

```
Ruijie(config)# bfd cpp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
10.3(4b3)	New command

bfd echo

Use this command to enable the echo mode in interface configuration mode.
Use the **no** form of this command to disable this function.
bfd echo
no bfd echo

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enbaled by default

Command Mode Interface configuration mode

Usage Guide By default, with BFD session parameters 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.*


Caution

This command cannot be configured on the L3 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 shows how to set the echo mode on the Routed Port FastEthernet 0/2:

```
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config)# no switchport (this command is not available for routers)
Ruijie(config-if)# bfd echo
```

Related Commands

Command	Description
bfd	Configures the BFD session parameters.
ip redirects	Enables the ICMP message redirection function.
bfd slow-timer	Configures the slow-timer time.

Platform Description N/A

Command History

Version	Description
10.3(4b3)	New command

bfd slow-timer

Use this command to enable the BFD ECHO function and set the slow timer, which is used to send the BFD control packets in the BFD asynchronous mode in global configuration mode.

Use the **no** form of this command to restore the default value.

bfd slow-timer [*milliseconds*]

no bfd slow-timer

Parameter Description

Parameter	Description
milliseconds	(Optional) BFD slow-timer time, in ms. The range is 1000 to 30000, and the default value is 1000ms.

Defaults 1000ms.

Command Mode Global configuration mode

Usage Guide -

Configuration Examples The following example sets the slow-timer as 14000ms:

```
Ruijie(config)# bfd slow-timer 14000
```

Related Commands

Command	Description
bfd echo	Enables the BFD echo function.

Platform Description N/A

Command History

Version	Description
10.3(4b3)	New command

bfd up-dampening

Use this command to set the bfd up-dampening time.

Use the **no** form of this command to restore the default value.

bfd up-dampening [*milliseconds*]

no up-dampening

Parameter Description

Parameter	Description
milliseconds	(Optional) bfd up-dampening time, in ms. In the range of 0-300000.

Defaults 0ms, which means that the session state is UP and sends notification about the application level of the state change immediately.

Command Mode Interface configuration mode

Usage Guide -

Configuration Examples The following example sets the bfd up-dampening time as 60000ms:

```
Ruijie(config)# bfd up-dampening 60000
```

Related Commands

Command	Description
bfd	Configures the BFD session parameters.

Platform Description N/A

Command History

Version	Description
10.3(4b3)	New command

bfd bind ldp-lsp, bfd bind static-lsp, bfd bind backward-lsp-with-ip

For details about the MPLS and BFD cooperation commands, refer to the *MPLS-CREF.doc*.

bfd bind peer-ip

Use this command to create a bfd session to cooperate with one interface status in interface configuration mode.
Use the **no** form of this command to remove this session.
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*	Peer IP address to be detected, which must directly connects to the Layer-3 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 as the uRPF at the same time
process-pst	Associates this session with the bdf status of the Layer-3 interface

Defaults N/A

Command Mode Interface configuration mode

Usage Guide Note that this command must be configured on the Layer-3 interface and the peer-ip detected must be the address directly-connected to the interface.

Configuration The following example detects the peer 1.1.1.2 through BFD on the routed port to generate the

Examples BFD status of the interface:

```
Ruijie(config)# interface FastEthernet 0/2
Ruijie(config-if)#no sw
Ruijie(config-if)#ip address 1.1.1.1 255.255.255.0
Ruijie(config-if)#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

Command History

Version	Description
10.3(4b3)	New command

ip ospf bfd

Use this command to configure the BFD for OSPF in interface configuration mode.
Use the **no** form of this command to remove this configuration.
ip ospf bfd [**disable**]
no ip ospf bfd

Parameter Description

Parameter	Description
disable	(Optional) Disables the configuration of BFD for OSPF on the interface.

Defaults BFD for OSPF is configured if the keyword **disable** is not input.

Command Mode Interface configuration mode

Usage Guide The following two methods are used to enable or disable the configuration of BFD for OSPF:
1. Use the **[no] bfd all-interfaces** command to enable or disable the configuration of BFD for the routing protocols on all interfaces in the OSPF routing configuration mode.
2. Use the **ip ospf bfd [disable]** command to enable or disable the configuration of BFD for OSPF on the specified interface in the interface configuration mode.

Configuration Examples The example below shows how to disable the configuration of BFD for OSPF on the Routed Port FastEthernet 0/2:

```
Ruijie(config)# interface FastEthernet 0/2
Ruijie(config-if)# no switchport (this command is not available for routers)
Ruijie(config-if)# ip ospf bfd disable
```

Related Commands

Command	Description
bfd	Sets the BFD session parameters.
bfd all-interfaces	Configures the BFD for the routing protocols on all interfaces.

Platform Description	N/A

Command History	**Version**	**Description**
	10.3(4b3)	New command

ip rip bfd

Use this command to configure the BFD for RIP in the interface configuration mode.
Use the **no** form of this command to remove this configuration.
ip rip bfd [**disable**]
no ip rip bfd

Parameter Description	**Parameter**	**Description**
	disable	(Optional) Disables the configuration of BFD for RIP on the interface.

Defaults	BFD for RIP is configured if the keyword **disable** is not input.
Command Mode	Interface configuration mode
Usage Guide	The following two methods are used to enable or disable the configuration of BFD for RIP: 1. Use the **[no] bfd all-interfaces** command to enable or disable the configuration of BFD for the routing protocols on all interfaces in the RIP routing configuration mode. 2. Use the **ip rip bfd [disable]** command to enable or disable the configuration of BFD for RIP on the specified interface in the interface configuration mode.

Configuration Examples	The example below shows how to disable the configuration of BFD for RIP on the Routed Port FastEthernet 0/2:
	`Ruijie(config)# interface FastEthernet 0/2`
	`Ruijie(config-if)# no switchport (this command is not available for routers)`
	`Ruijie(config-if)# ip rip bfd disable`

Related Commands	**Command**	**Description**
	bfd	Sets the BFD session parameters.
	bfd all-interfaces	Configures the BFD for the routing protocols on all interfaces.

Platform Description	N/A

Command History	**Version**	**Description**
	10.3(4b3)	New command

ip route static bfd

Use this command to configure the BFD for the static route in global configuration mode.

Use the **no** form of this command to remove this configuration.

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*]

Parameter Description

Parameter	Description
vrf *vrf-name*	(Optional) Sets the VRF name of the static router.
interface-type interface-number	Sets the interface type and interface number.
gateway	Sets the IP address for the gateway, which is the neighbor IP address for BFD. The static route next-hop of the neighbor detects the reachability of the forwarding path through BFD.
source *ip-address*	(Optional) Sets the source IP address for the BFD session. It is necessary to set this parameter if the distance between the session IP address and the neighbor IP address are multi-hops.

Defaults

No BFD is configured for the static route.

Command Mode

Global configuration mode

Usage Guide

Note that the BFD session parameters must be configured before the configuraiton.

Configuration Examples

The following example shows how to configure the BFD for the static routes and detects the forwarding path between the neighbor 172.16.0.2 through BFD:

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# no switchport (this command is not available for routers)
Ruijie(config-if)# ip address 172.16.0.1 255.255.255.0
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)# ip route static bfd FastEthernet 0/1 172.16.0.2
Ruijie(config-if)# ip route 10.0.0.0 255.0.0.0 FastEthernet 0/1 172.16.0.2
```

Related Commands

Command	Description
bfd	Sets the BFD session parameters.

Platform Description

N/A

Command

Version	Description

History	10.3(4b3)	New command

ipv6 ospf bfd

Use this command to configure BFD support for OSPFv3 in interface configuration mode.
Use the **no** form of this command to remove this configuration.
ipv6 ospf bfd [**disable**] [**instance** *instance-id*]
no ipv6 ospf bfd [**disable**] [**instance** *instance-id*]

Parameter Description

Parameter	Description
disable	(Optional) Disables BFD support for OSPFv3 on the interface.
instance *instance-id*	(Optional) Configures an OSPFv3 instance, in the range from 0 to 255.

Defaults BFP support for OSPFv3 is not configured by default.

Command Mode Interface configuration mode

Usage Guidle The **ipv6 ospf bfd** command prevails over the **bfd all-interfaces** command. You can select either command to enable BFD.
1. Use the [**no**] **bfd all-interfaces** command to enable or disable BFD support for OSPF on all interfaces in the OSPF routing configuration mode.
2. Use the **ip ospf bfd** [**disable**] command to enable or disable BFD support for OSPF on the specified interface in the interface configuration mode.

Configuration Examples The following example disables BFD support for OSPFv3 on Routed Port FastEthernet 0/2:

```
Ruijie(config)# interface FastEthernet 0/2
Ruijie(config-if)# ipv6 ospf bfd disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 route static bfd

Use this command to configure the BFD for the static route in global configuration mode.
Use the **no** form of this command to remove this configuration.
ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]

no ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]

Parameter Description

Parameter	Description
vrf *vrf-name*	(Optional) Sets the VRF name of the static router.
interface-type interface-number	Sets the interface type and interface number.
gateway	Sets the IP address for the gateway, which is the neighbor IP address for BFD. The static route next-hop of the neighbor detects the reachability of the forwarding path through BFD.
source *ipv6-address*	(Optional) Sets the source IP address for the BFD session. It is necessary to set this parameter if the distance between the session IP address and the neighbor IP address are multi-hops.

Defaults No BFD is configured for the static route.

Command Mode Global configuration mode

Usage Guide Note that the BFD session parameters must be configured before the configuraiton.

Configuration Examples The following example configures the BFD for the static routes and detects the forwarding path between the neighbor *2001:1::2* through BFD:

```
Ruijie(config)# interface FastEthernet 0/1
Ruijie(config-if)# ip address 2001:1::1/64
Ruijie(config-if)# bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)# ipv6 route static bfd FastEthernet 0/1 2001:1::2
Ruijie(config-if)# ipv6 route 2002::/64 FastEthernet 0/1 2001:1::2
```

Related Commands

Command	Description
bfd	Sets the BFD session parameters.

Platform Description N/A

Command History

Version	Description
10.4(1)	Supports evaluation.
10.4(3)	Supports VRF parameter.

isis bfd

Use this command to configure BFD support for ISIS in interface configuration mode.
Use the **no** form of this command to remove this configuration.
isis bfd [**disable**]
no isis bfd [**disable**]

Parameter Description

Parameter	Description
disable	(Optional) Disables BFD support for ISIS on the interface.

Defaults

If the **bfd all-interfaces** command is configured, BFP support for ISIS is enabled by default.

Command Mode

Interface configuration mode

Usage Guidle

The **isis bfd** command prevails over the **bfd all-interfaces** command. You can select either command to enable BFD.
1. Use the [**no**] **bfd all-interfaces** command to enable or disable BFD support for ISIS on all interfaces in the ISIS routing configuration mode.
2. Use the **isis bfd** [**disable**] command to enable or disable BFD support for ISIS on the specified interface in the interface configuration mode.

Configuration Examples

The following example disables BFD support for ISIS on Routed Port FastEthernet 0/2:

```
Ruijie(config)# interface FastEthernet 0/2
Ruijie(config-if)# isis bfd disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

neighbor fall-over bfd

Use this command to configure the BFD for BGP to detect the change of the specified neighbor to speed up the BGP convergence in the route or addres-family configuration mode.
Use the **no** form of this command to disable this function.
neighbor *ip-address* **fall-over bfd**
no neighbor *ip-address* **fall-over bfd**

Parameter Description

Parameter	Description
ip-address	Specifies the BGP neighbor.

Defaults No BFD is configured for BGP.

Command Mode Route or address-family configuration mode

Usage Guide Note that the BFD session parameters must be configured before the configuraiton.

Configuration Examples The following example shows how to configure the BFD for BGP to detect the forwarding path between the neighbor 172.16.0.2 through BFD:

```
Ruijie(config)# routerbgp 44000
Ruijie(config-router)# bgp log-neighbors-changes
Ruijie(config-router)# neighbor 172.16.0.2 remote-as 45000
Ruijie(config-router)# neighbor 172.16.0.2 fall-over bfd
Ruijie(config-router)# end
```

Related Commands

Command	Description
bfd	Sets the BFD session parameters.

Platform Description N/A

Command History

Version	Description
10.3(4b3)	New command

set ip next-hop verify-avalability

Use this command to configure the BFD for PBR to detect whether the next-hop of the configured PBR is valid or not by the Track method.

Use the **no** form of this command to disable this function.

set ip next-hop verify-availability [*next-hop-address* [**track** *number*|**bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*]]

no set ip next-hop verify-availability [*next-hop-address* [**track** *number*|**bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*]]

Parameter Description

Parameter	Description
vrf *vrf-name*	(Optional) Sets the VRF name of the static router.
next-hop-address	(Optional) Sets the next-hop IP address.
track	(Optional) Determines whether the next-hop is valid or not by the Track method.
number	(Optional) Track object number
bfd	(Optional) Neighbor detection by the BFD method
interface-type interface-number	(Optional) Sets the interface type and interface number.

gateway	(Optional) Sets the IP address for the gateway, which is the neighbor IP address for BFD. The static route next-hop of the neighbor detects the reachability of the forwarding path through BFD.

Defaults No BFD is configured for PBR.

Command Mode Route-map configuration mode

Usage Guide

Note that the BFD session parameters must be configured before the configuraiton.

Configuration Examples The following example shows how to configure the BFD for PBR to detect the forwarding path between the neighbor 172.16.0.2 through BFD:

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# route-map Example1 permit 10
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set ip precedence priority
Ruijie(config-route-map)#set ip next-hop verify-availability 172.16.0.2
bfd FastEthernet 0/1 172.16.0.2
Ruijie(config-route-map)#end
```

Related Commands

Command	Description
bfd	Sets the BFD session parameters.

Platform Description N/A

Command History

Version	Description
10.3(4b3)	New command

set ipv6 next-hop verify-availability

Use this command to enable BFD support for PBR to detect the IPv6 address of the neighbor and check whether the next-hop of the configured PBR is valid or not. Use the **no** form of this command to disable this function.

set ipv6 next-hop verify-availability *next-hop-ipv6-address* **bfd** *interface-type interface-number ipv6-gateway*

no set ipv6 next-hop verify-availability *next-hop-ipv6-address* **bfd** *interface-type interface-number ipv6-gateway*

Parameter Description

Parameter	Description
vrf *vrf-name*	(Optional) Sets the VRF name of the static router.
next-hop-address	(Optional) Sets the next-hop IPv6 address.
bfd	(Optional) Neighbor detection by the BFD method
interface-type interface-number	(Optional) Sets the interface type and interface number.
ipv6-gateway	(Optional) Sets the IPv6 address for the gateway, which is the neighbor IPv6 address for BFD. The static route next-hop of the neighbor detects the reachability of the forwarding path through BFD.

Defaults

BFD support for PBR is disabled by default.

Command Mode

Route-map configuration mode

Usage Guide

Note

Make sure that the BFD session parameters must be configured before the configuraiton.

Configuration Examples

The following example enables BFD support for PBR to detect the forwarding path between the neighbor 2001:1::2 through BFD:

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# route-map Example1 permit 10
Ruijie(config-route-map)# match ipv6 address 1
Ruijie(config-route-map)# set ipv6 precedence priority
Ruijie(config-route-map)#set  ipv6  next-hop  verify-availability
2001:1::2 bfd FastEthernet 0/1 2001:1::2
Ruijie(config-route-map)#end
```

Related Commands

Command	Description
bfd	Sets the BFD session parameters.

Platform Description

N/A

Command History

Version	Description
10.3(4b3)	New command

vrrp bfd

Use this command to configure the BFD for VRRP to detect whether the master router is active or not in interface configuration mode.

Use the **no** form of this command to disable this function.

vrrp *group-number* **bfd** *ip-address*

no vrrp *group-number* **bfd** *ip-address*

Parameter Description

Parameter	Description
group-number	Configures the BFD for the specified VRRP group to detect whether the master router is active or not.
Ip-address	Specifies the neighbor IP address.

Defaults

By default, VRRP does not detect whether the master or backup router is active or not through BFD.

Command Mode

Interface configuration mode

Usage Guide

Note

that the BFD session parameters must be configured before the configuraiton.

If multiple routers exist in the VRRP group, it is a necessity to use this command to set the neighbor IP address for all possible backup routers.

Configuration Examples

The following example shows how to configure the BFD for VRRP to detect the forwarding path between the master and backup routers 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 (this command is not available for routers)
Ruijie(config-if)#ip address 192.168.201.11 255.255.255.0
Ruijie(config-if)#bfd interval 50 min_rx 50 multiplier 3
Ruijie(config-if)#vrrp 1 priority 120
Ruijie(config-if)#vrrp 1 ip 192.168.201.1
Ruijie(config-if)#vrrp 1 bfd 192.168.201.12
Ruijie(config-if)#end
```

Related Commands

Command	Description
bfd	Sets the BFD session parameters.

Platform Description

N/A

Command History	Version	Description
	10.3(4b3)	New command

show bfd neighbors

Use this command to show the BFD session parameters.

show bfd neighbors [**vrf** *vrf-name*] [**ipv4** *ip-addess* [**details**]| **ipv6** *ip-addess* [**details**] | **client** { **bgp | ospf | rip | vrrp | static-route | ldp-lsp | static-lsp | backward-lsp-with-ip | pst**} [**ipv4** *ip-addess* [**details**] | **ipv6** *ip-addess* [**details**]| **details**]]

Parameter Description

Parameter	Description
vrf *vrf-name*	(Optional) Sets the neighbor VRF name.
client	(Optional) Specifies the routing protocol.
bgp	Shows the BFD session configuration for BGP.
ospf	Shows the BFD session configuration for OSPF.
rip	Shows the BFD session configuration for RIP.
vrrp	Shows the BFD session configuration for VRRP.
static-route	Shows the BFD session configuration for the static route.
pbr	Shows the BFD session configuration for PBR.
ldp-lsp	Shows the BFD session configuration for the LDP-LSP.
backward-lsp-with-ip	Shows the BFD session configuration for the LSP backward IP cooperation.
static-lsp	Shows the BFD session configuration for the static LSP cooperation.
pst	Shows the BFD session configuraiton and the layer-3 interface status.
ipv4 *ip-address*	Shows the session information of the specified IPv4 neighbor.
ipv6 *ip-address*	Shows the session information of the specified IPv6 neighbor.
details	Shows the configurations in detail.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

Note In the command output of show bfd neighbors, OurAddr indicates the source session address. If the value is "—", no source address has been specified. This information will be displayed in the LSP reverse IP BFD session.

Configuration Examples

```
#The following example shows the result of the command show bfd neighbors:
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

#The following example shows the result of the command show bfd neighbors details:
Ruijie# show bfd neighbors details
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
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 Registered protocols: BGP
Uptime: 02:18:49
Last packet: Version: 1             - Diagnostic: 0
I Hear You bit: 1          - Demand bit: 0
Poll bit: 0            - Final bit: 0
Multiplier: 3          - Length: 24
My Discr.: 2       - Your Discr.: 1
Min tx interval: 50000     - Min rx interval: 50000
Min Echo interval: 0
```

Field	Description
OurAddr	Local IP address
NeighAddr	Neighbor IP address
LD/RD	Local & Remote identifiers
RH/RS	Current state of the peer end in the session
Holdown(mult)	Time of not receiving the hello packets for the local session and the times of the timeout detection
State	Current session state
Int	Interface number for the session
Session state is UP and using echo function with 50 ms interval	Whether the session is in echo mode and the echo interval (which is shown only in 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	Minimum sending interval for the local session
MinRxInt	Minimum receiving interval for the local session
Multiplier	Timeout detection times for the local session

Received MinRxInt	Minimum sending interval for the remote session
Received Multiplier	Timeout detection times for the remote session
Holdown (hits)	Session detection time and the times of the timeout detection
Hello (hits)	Minimium interval of receiving the hello packets after the session negotiation
Rx Count	Number of BFD packets received by the local session
Rx Interval (ms) min/max/avg	Minimum, maximum and average intervals of receiving for the local session
Tx Count	Number of BFD packets sent by the local session
Tx Interval (ms) min/max/avg	Minimum, maximum and average intervals of sending for the local session
Registered protocols	Registered protocol type of the session
Uptime	Time of keeping the session UP
Last packet	Last BFD packet information received by the local session

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Command History

Version	Description
10.3(4b3)	New command

Dialing Configuration Commands

Dialing Commands

async mode

Use this command to specify the asynchronous dialup mode.
Use the **no** form of this command to restore the default setting.
async mode dedicated
no async mode

Parameter Description

Parameter	Description
dedicated	Automatic asynchronous dialup mode

Defaults The asynchronous dialup mode is not set by default.

Command Mode Interface configuration mode

Usage Guide This command is used to specify the asynchronous dialup mode.

Configuration Examples The following example sets the dialup mode of asynchronous interface 1 as the automatic asynchronous dialup mode:

```
Ruijie(config)# interface async 1
Ruijie(config-if)# async mode dedicated
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

backup load

Use this command to set the bandwidth percentage when the backup interface is enabled or disabled.
Use the **no** form of this command to restore the setting to the default value.
backup load { *enable-delay-percent* **| never** } {*disable-delay-percent* **| never** }

no backup load

Parameter Description

Parameter	Description
enable-delay-percent	Maximum bandwidth percentage of the master interface when the backup interface is enabled, namely the percentage by which the master interface link must be higher than its maximum available bandwidth
disable-delay-percent	Maximum bandwidth percentage of the master interface when the backup interface is disabled, namely the percentage by which the master interface link must be lower than its maximum available bandwidth
never	The system neither changes the backup state of the backup interface (active or standby) nor enables or disables the backup interface.

Defaults No bandwidth percentage of backup interface is set by default.

Command Mode Interface configuration mode

Usage Guide When the bandwidth percentage of the maximum available bandwidth consumed by the traffic on the master interface exceeds the one set by the *enable-delay-percent* parameter, loads are balanced on the backup interface. On the other hand, when the bandwidth percentage of the maximum available bandwidth consumped by the traffic on the master interface and the backup interface is lowered than the one set by the *disable-delay-percent* parameter, the system disables the backup interface link and sets it to standby. Note that this command takes effect only after the backup interface is set on the master interface.

Configuration Examples The following example sets the bandiwdth percentage on Serial 1/0 for enabling or disabling the backup interface. When the bandwidth consumed by the traffic on the master interface exceeds 70% of the maximum available bandwidth, the systme enables the backup interface link for load balancing. When the bandwidth percentage of the maximum available bandwidth of the master interface consumed by the traffic on the master interface and the backup interface is lower than 10%, the system sets the backup interface to standby.

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# backup load 10 70
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

clear counters

Use this command to clear the interface statistics.

clear counters [*interfece-type interface-number*]

Parameter Description

Parameter	Description
interface-type	Interface type, including Async, Dialer, FastEthernet, Group-Async, Loopback, Null and Serial
interface-number	Number of interface.

Command Mode Privileged EXEC mode

Usage Guide The statistics of an interface is displayed by using **show interface**. This command is used to clear the statistics of the interface for line debugging purpose.

Configuration Examples The following example shows the output of the command.

```
Ruijie# show interface async 1
Async1 is down, line protocol is down
Hardware is Async Serial
Internet address is 1.1.1.1/24
MTU 1500 bytes, BW 9 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive not set
DTR is pulsed for 5 seconds on reset
LCP Closed
Closed: ipcp
Last input 18:17:02, output 18:17:02, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/64/0 (size/threshold/drops)
Conversations  0/1 (active/max active)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1396 packets input, 20516 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
1 input errors, 1 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1467 packets output, 22937 bytes, 0 underruns
0 output errors, 0 collisions, 11 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
Ruijie# clear  counters
Clear "show interface" counters on all interfaces [confirm]
Ruijie#
%COUNTERS: Clear counter on all interfaces by console
Ruijie# show interface async 1
Async1 is down, line protocol is down
Hardware is Async Serial
Internet address is 1.1.1.1/24
MTU 1500 bytes, BW 9 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive not set
DTR is pulsed for 5 seconds on reset
LCP Closed
Closed: ipcp
Last input 18:17:15, output 18:17:15, output hang never
Last clearing of "show interface" counters 00:00:02
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/64/0 (size/threshold/drops)
Conversations  0/1 (active/max active)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

Related Commands

Command	Description
show interface	Shows the interface statistic information.

Platform Description

N/A

Command History

Version	Description
N/A	N/A

clear interface

Use this command to clear the hardware logical information of an interface.

clear interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type	Interface type, including Async, Dialer, FastEthernet, Group-Async, Loopback, Null and Serial
interface-number	Number of interface

Command Mode Privileged EXEC mode

Configuration Examples The following example clears the hardware logical information of serial interface 0:

```
Ruijie# clear interface serial  1/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer callback-secure

Use this command to make sure that callback is performed only for the authenticated remote host.

Use the **no** form of this command to cancel the callback security authentication.

dialer callback-secure

no dialer callback-secure

Parameter Description

Parameter	Description
N/A	N/A

Defaults Callback security authentication is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command ensures that callback is performed only for remote hosts that pass authentication and have had their host user names configured by running **dialer map**.

Configuration Examples The following example configures callback for the remote host named Myremote on the device:

```
Ruijie(config)# interface async 1
Ruijie(config-if)# dialer map ip 1.1.1.1 name myremote class dial
Ruijie(config-if)# dialer callback-secure
```

Related Commands

Command	Description
dialer callback-server	Enables the callback function after successful negotiation.
dialer map	Configures the interface dialup destination mapping.
map-class dialer	Configures the dialup mapping class.
ppp callback	Configures the interface as the callback client or server.

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer callback-server

Use this command to configure the ppp callback reference.
Use the **no** form of this command to cancel the callback server.
dialer callback-server {dial-string | username}
no dialer callback-server

Parameter Description

Parameter	Description
dial-string	Performs callback according to the number configured in the global *username*.
username	Performs callback according to the *name* parameter in *dialer map*.

Defaults Ppp callback function is not configured.

Command Mode Map-class dialer configuration mode

Usage Guide The two parameters can be both configured, but only the **username** parameter is supported on our device currently.

Configuration The following example configures the interface bri0 as the callback server and the reference is the

Examples **name** in the **dialer map**.

```
interface BRI0
 ip address 172.19.1.9 255.255.255.0
 encapsulation ppp
 dialer callback-secure
 dialer enable-timeout 2
 dialer map ip 172.19.1.8 name myremote class dial1 81012345678901
dialer-group 1
ppp callback accept
 ppp authentication chap
!
map-class dialer dial1
 dialer callback-server username
```

Related Commands

Command	Description
dialer map	Configures the interface dialup destination mapping.
map-class dialer	Configures the dialup mapping class.
ppp callback	Configures the interface as the callback client or server.

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer enable-timeout

Use this command to set line invalid time.

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

dialer enable-timeout *seconds*

no dialer enable-timeout

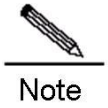
Parameter Description

Parameter	Description
senconds	Line invalid time (seconds)

Defaults 15 seconds

Command Mode Interface configuration mode

Usage Guide The line invalid time is the time that the interface needs to wait before dialup after line disconnection or dialup failure,



Note

On the callback server, the callback start time is **dialer enable-timeout +2 seconds**. Therefore, in actual application, ensure that the value of **dialer enable-timeout** is greater than the value of **dialer idle-timeout** by 2 seconds. Otherwise, callback will not work,

Configuration Examples The following example specifies the line invalid time as 10 seconds:

```
Ruijie(config)# interface async 1
Ruijie(config-if)# dialer enable-timeout  10
```

Related Commands

Command	Description
dialer idle-timeout	Sets the idle time of the line.

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer-group

Use this command to associate the dialup stimulation rule on the interface.
Use the **no** form of this command to remove the association.
dialer-group *group-number*
no dialer-group

Parameter Description

Parameter	Description
group-number	Number of dialup stimulation rule

Defaults No dialup rule is associated by default.

Command Mode Interface configuration mode

Usage Guide If an interface attempts to dial up, it is necessary to determine what kind of messages can stimulate dialup. The dialup stimulation rule is specified by using a global configuration command **dialer-list**. Then, a dialup rule is associated on the interface.

Configuration Examples The following example associates the dialup stimulation rule 1 (only IP packets can stimulate dialup):

```
Ruijie(config)# dialer-list  1 protocol  ip permit
Ruijie(config)# interface async 1
Ruijie(config-if)# dialer-group 1
```

Related Commands

Command	Description
dialer-list	Defines dialup rules.

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer hold-queue

Use this command to configure the hold queue of the interface.
Use the **no** form of this command to close the hold queue.
dialer hold-queue *packets* [**timeout** *seconds*]
no dialer hold-queue [*packets* [**timeout** *seconds*]]

Parameter Description

Parameter	Description
packet	Packets of the hold messages in the queue, ranging from 0 to 100
timeout *seconds*	Sets the packet holding time in the queue (in seconds).

Defaults Hold queue is closed.

Command Mode Interface configuration mode

Usage Guide A period of negotiation is needed when the device works with MODEM to dial, during which messages may be dropped. If the hold queue is configured, it is possible to configure the stimulation dialup rule messages to hold on the device and will be sent up on the setup of connection.

Configuration Examples The following example configures the hold queue timeout as 50:

```
Ruijie(config)# interface async 1
Ruijie(config-if)# dialer hold-queue 50
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer-list

Use this command to define the rule to stimulate dialup.

Use the **no** form of this command to delete the specified stimulation dialup rule.

dialer-list *dialer-group* **protocol** { **ip** } { **permit** | **deny** | **list** *access-list-number* }

no dialer-list *dialer-group* [**protocol** { **ip** } { **permit** | **deny** | **list** *access-list-number* }]

Parameter Description

Parameter	Description
dialer-group	Number of the stimulated dialup rule
permit	Allows the whole protocol.
deny	Rejects the whole protocol.
list	Usse the access list instead of the whole protocol to define the stimulation dialup rule.
access-list-number	Number of the access list

Defaults Stimulation dialup rule is not defined by default.

Command Mode Global configuration mode.

Usage Guide This command in the global configuration mode defines one or more stimulation dialup rule(s). The **dialer-group** command applies the dialup rule on the specific interface dialup. It is one of the necessary commands for outgoing dialup.

Configuration Examples The following example defines two rules to stimulate dialup: one allows all IP messages to stimulate dialup; the other allows only the messages that match access list 120 to stimulate dialup.

```
Ruijie(config)# access-list 120 permit tcp
192.168.11.0 0.0.0.255 192.168.12.0 0.0.0.255
Ruijie(config)# dialer-list 1 protocol ip permit
Ruijie(config)# dialer-list 2 protocol ip list 120
```

Related Commands

Command	Description
dialer-group	Associates the stimulation dialup rule on the interface.
access-list	Defines the access list.

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer map

Use this command to configure the interface for dialing to connect with multiple destination addresses.

Use the **no** form of this command to delete the specified destination address dialup mapping.

dialer map *protocol next-hop-address* [**name** *host-name*] [**broadcast**] [**modem-script** *script-name*] [**system-script** *script-name*] [*dial-string*][**class** *map-class-name*]

no dialer map *protocol next-hop-address* [**name** *host-name*] [**broadcast**] [**modem-script** *script-name*] [**system-script** *script-name*] [**class** *map-class-name*]

Parameter Description

Parameter	Description
protocol	Including IP
next-hop-address	Dialup next-hop address
name *host-name*	Specifies the remote hostname; connection is disconnected if hostname does not matches.
broadcast	Broadcast message
modem-script *script-name*	Specifies the dialup script.
system-script *script-name*	Specifies the remote login script.
class *map-class-name*	Specifies the callback dialup mapping class.

Defaults No dialup mapping is specified by default.

Command Mode Interface configuration mode

Usage Guide To use the device for dialup, the **dialer string** or **dialer map** command can be used to define the destination telephone number. They are mutually exclusive and only one of them can be configured at a time. In the following cases, it is necessary to use **dialer map** for dialup:

- Legacy DDR
- Call-back

The **dialer map** accepts specifying the dialup script. In the line configuration mode, the **script dialer** also accepts specifying dialup script. If the dialup scripts are used for both commands, the two scripts must be the same to allow dialup.

The **class** option is used only in case of callback.

Note If the link protocol encapsulation is SLIP, dialer map is not supported.

Configuration Examples

The following example configures the asynchronous interface 1 to use telephone number 68934113 to initiate the dialup connection request when receiving the message with next-hop address 1.1.1.1 (hostname as remote) and compliant with the stimulation dialup rule:

```
Ruijie(config)# chat-script Dialout ABORT BUSY ABORT ERROR """AT Z"OK "ATDT\T" TIMEOUT 40 CONNECT \c
Ruijie(config)# interface async 1
Ruijie(config-if)# dialer map ip 1.1.1.1 name remote modem-script Dialout 68934113
```

Related Commands

Command	Description
chat-script	Defines the dialup script.

Platform Description

N/A

Command History

Version	Description
N/A	N/A

dialer pool-member

Use this command to add the physical interface into the specified dialer pool.
Use the **no** form of this command to delete the association between the physical interface and the dialer pool.
dialer pool-member *number* [**priority** *priority*]
no dialer pool-member *number* [**priority** *priority*]

Parameter Description

Parameter	Description
number	Number of the dialer pool
priority *priority*	Specifies the priority (0 - 255) of a physical interface in the dialer pool, 0 for the lowest priority and 255 for the highest priority. The logical interface first uses the idle physical interface with the highest priority in the dialer pool for dialup.

Defaults

Physical interface is not added into the dialer pool. The priority is 0 by default.

Command Mode

Interface configuration mode

Usage Guide This command adds a physical interface into the specified dialer pool, which is available for the logical interface to dial up.
One physical interface can be added into multiple dialer pool, with a priority specified in each dialer pool. The logical interface first uses the idle physical interface with the highest priority in the dialer pool for dialup.

Configuration Examples The following example adds the physical asynchronous interface 1 into dialer pools 1 and 2, with priorities 50 and 100 respectively:

```
Ruijie(config)# interface async 1
Ruijie(config-if)# dialer pool-member 1 priority 50
Ruijie(config-if)# dialer pool-member 2 priority 100
```

Related Commands

Command	Description
dialer pool	Associates the dialer pool on the logical interface.
dialer remote-name	Specifies the remote hostname.

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer watch-group

This command implements the dialup backup function on the interface. Use this command to determine whether to enable the backup line by viewing the watch-list route changes.
Use the **no** form of this command to restore the default setting.
dialer watch-group *group-number*
no dialer watch-group *group-number*

Parameter Description

Parameter	Description
group-number	Watch-list number of the IP address list for route backup, ranging from 1 to 255

Defaults N/A

Command Mode Interface configuration mode

Usage Guide The configuration of this command determines which interface will be implemented with the DDR dialup backup. The interface with this command is the backup interface. Watch the related watch-list IP address route change of the interface to determine whether to enable the backup interface.

Configuration Examples The following example enable the watch-list dialup backup on the ADYNC 1 interface, where the watched list number is 1:

```
interface async 1
ip address 10.1.1.2 255.255.255.0
encapsulation ppp
dialer watch-group 1
```

Related Commands

Command	Description
dialer watch-list	Configures the watch-list address list.

Platform Description N/A

Command History

Version	Description
N/A	N/A

dialer watch-list

Use this command to define a series of watch lists of IP address routes.

dialer watch-list *group-number* {**ip** *ip-address address-mask*}

no dialer watch-list *group-number* {**ip** *ip-address address-mask*}

Parameter Description

Parameter	Description
group-number	Watch-list number of the IP address list for route backup, ranging from 1 to 255
ip *ip-address address-mask*	Related IP address mask for the IP address range to be watched. The route change of that IP address range will trigger dialup backup events.

Defaults None

Command Mode Global configuration command mode

Usage Guide This command determines the route changes of which IP address range will be watched. When the **dialer watch-group** command is related with this command, it is possible to enable the dialup backup function according to route changes.

Configuration Examples

The following example watches the route changes of 2.2.2.0 and 3.3.3.0 network segments. If the F0/0 interface is disconnected and causes the loss of 2.2.2.0 route, it will results in the dialup behavior of the ADYNC 1 backup interface.

```
dialer watch-list 1 ip 2.2.2.0 255.255.255.0
dialer watch-list 1 ip 3.3.3.0 255.255.255.0
interface FastEthernet 0/0
ip address 2.2.2.1 255.255.255.0
ip address 3.3.3.1 255.255.255.0 secondary
interface async 1
ip address 10.1.1.2 255.255.255.0
async mode dedicate
encapsulation ppp
dialer in-band
dialer string 3001
dialer watch-group 1
```

Related Commands

Command	Description
dialer watch-group	Associates the watch-list command on the interface.

Platform Description

N/A

Command History

Version	Description
N/A	N/A

dialer watch-list delay

Use this command to define the time interval between the enablement and disconnection of the dialup backup interface.

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

dialer watch-list *group-number* **delay** {**connect** *connect-time* | **disconnect** *disconnect-time*}

no dialer watch-list *group-number* **delay** {**connect** *connect-time* **| disconnect** *disconnect-time*}

Parameter Description

Parameter	Description
group-number	Watch-list number of the IP address list for route backup, range 1 - 255
connect *connect-time*	Performs the dial on the backup line in the duration connect-time after the router watched by the watch-list is lost
disconnect *disconnect-time*	Disconnects the dial on the backup line in the duration connect-time after the router watched by the watch-list appears.

Defaults

connect-time and *disconnect-time* are 0.

Command Mode Global configuration mode

Usage Guide This command determines when to enable and disconnect the dial update line. When the **dialer watch-group** command is related with this command, it is possible to execute the dialup backup function according to the route changes.

Configuration Examples The following example watches the route changes of 2.2.2.0 and 3.3.3.0 network segments. If the F0/0 interface is disconnected and causes the loss of 2.2.2.0 route, it will results in the dialup behavior of the ASYNC 1 backup interface. The dialup backup interface is enabled in 10 seconds since the loss of the master router, and the dialup backup interface is disconnected in 20 seconds since the master route appears.

```
dialer watch-list 1 ip 2.2.2.0 255.255.255.0
dialer watch-list 1 ip 3.3.3.0 255.255.255.0
dialer watch-list 1 delay connect 10
dialer watch-list 1 delay disconnect 20
interface FastEthernet 0/0
ip address 2.2.2.1 255.255.255.0
ip address 3.3.3.1 255.255.255.0 secondary
interface async 1
ip address 10.1.1.2 255.255.255.0
async mode dedicate
encapsulation ppp
dialer in-band
dialer string 3001
dialer watch-group 1
```

Related Commands

Command	Description
dialer watch-group	Associates the watch-list command on the interface.

Platform Description N/A

Command History

Version	Description
N/A	N/A

ip address negotiate

Use this command to configure the address to obtain address via PPP negotiation.
Use the **no** form of this command to cancel this function.
ip address negotiate
no ip address negotiate

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is mostly used for the dialup remote client so that the IP address of the remote client is dynamically allocated by the server, to make management easier and save address resources.

Configuration Examples The following example configures the asynchronous interface 1 to obtain IP address via negotiation:

```
Ruijie(config)# interface async 1
Ruijie(config-if)# ip address  negotiate
```

Related Commands

Command	Description
encapsulation ppp	Encapsulates PPP protocol.
ip address	Specifies the IP address of the interface.
ip unnumbered	Shares the other interface IP address.

Platform Description N/A

Command History

Version	Description
N/A	N/A

ip address-pool

Use this command to define the global IP address allocation policy.
Use the **no** form of this command to restore the default setting.
ip address-pool [**local**]
no ip address-pool

Parameter Description

Parameter	Description
local	Local address allocation policy, using the local default IP address pool to allocate IP address of the dial-in users

Defaults Global address allocation policy is not specified.

Command Mode Global configuration mode

Usage Guide This command specifies the default address allocation policy for the dial-in users. In the following cases, the global address allocation policy is overwritten:
Use the **peer default ip address** command to specify address or address pool for the dial-in user on the interface.

Configuration Examples The following example specifies the global address allocation policy to use the local default address pool:

```
Ruijie(config)# ip address-pool local
```

Related Commands

Command	Description
ip local pool	Defines local address pool.
peer default ip address	Specifies the IP address of the dial-in user.

Platform Description N/A

Command History

Version	Description
N/A	N/A

ip route

For the details of the command, see the *IP Protocol Command Reference*.

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

Command History

Version	Description
N/A	N/A

line

Use this command to enter the specified line configuration mode to customize the line parameters.

line [**aux** | **console** | **vty**] *line-number* [*ending-line-number*]

Parameter Description

Parameter	Description
aux	Line terminal line corresponding to the backup interface
console	Line terminal line corresponding to the console
vty	Virtual terminal line provided for remote access
line-number	Line number; the number of the first line in case of continuous configuration group
end-line-number	Number of the last line in a continuous configuration group

Defaults No default line terminal line

Command Mode Global configuration mode

Usage Guide This command allows configuring an individual line or a group of lines. If no **aux \ console \ vty** keyword follows Line, the number parameter means absolute numbering, which can be seen by using the **show line** command.

```
Ruijie# sh line 1
Tty    Type    speed   Overexecutes
* 0    AUX    115200  0
Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
^^x    none       ^M
Timeouts:     Idle EXEC    Idle Session
00:10:00    never
History is enabled, history size is 10.
Total input: 0 bytes
Total output:  1 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times
Modem: IDLE
```

The number below TTY is an absolute number. The number of the console is always 0. The number of the other interfaces changes with the insertion of the asynchronous cards, which can be seen by using the **show line** command.

In case of no **aux \ console \ vty** keyword, the line number is generally the same as the number of the asynchronous interface. That is, the line number of the asynchronous interface 1 is 1. For different versions, see the **show line** command or the current version configuration guide.

Configuration Examples The following example enters into virtual lines 0 - 4 configuration group to configure parameters. The configured parameters apply on virtual lines 0 - 4:

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)# exec-timeout 0 0
```

Related Commands

Command	Description
show line	Displays the line information.

Platform Description N/A

Command History

Version	Description
N/A	N/A

map-class dialer

Use this command to define a dialup mapping class that contains common configurations for the callback or **dialer map**.
Use the **no** form of this command to delete the specified mapping class.
map-class dialer *class-name*
no map-class dialer *class-name*

Parameter Description

Parameter	Description
class-name	Name of the dialup mapping class

Defaults No default dialup mapping class

Command Mode Global configuration mode

Usage Guide Only the callback server needs the definition of dialup mapping class. The **class** name used in the **dialer map** configuration command for the callback server interface shall be one-to-one corresponding to the dialup mapping class name.
The dialup mapping class defines some common configurations available for the use of specific dialup.

Configuration Examples The following example defines a dialup mapping class for the callback server.

```
Ruijie(config)# map-class dialer callbackclass
Ruijie(config-map-class)# dialer callback-server
Ruijie(config-map-class)# exit
Ruijie(config)# interface async 1
Ruijie(config-if)# dialer map ip 1.1.1.2 name Client class Callbackclass 689341
Ruijie(config-if)# ppp callback accept
```

Related Commands

Command	Description
dialer map	Configures the dialup mapping class.
ppp callback	Configures the callback options.

Platform Description N/A

Command History

Version	Description
N/A	N/A

modem dialin

Use this command to configure the MODEM connected on the device to accept dial-in only.
Use the **no** form of this command to cancel this function.
modem dialin
no modem dialin

Defaults Dial-in is not accepted.

Command Mode Line configuration mode

Usage Guide This command makes the MODEM on the router accept dial-in only but disallow dial-out. To allow the MODEM to accept both dial-in and dial-out, execute the line configuration command **modem inout**.

Configuration Examples The following example makes the MODEM connected on the router accept dial-in only.

```
Ruijie(config)# line aux 0
Ruijie(config-line)# modem dialin
```

Related Commands

Command	Description
modem inout	Configures the line to accept both dial-in and dial-out.

Platform Description N/A

Command History

Version	Description
N/A	N/A

modem inout

Use this command to configure the line to accept both dial-in and dial-out.
Use the **no** form of this command to cancel this function.
modem inout
no modem inout

Defaults No MODEM control; The MODEM does not dial in or out.

Command Mode Line configuration mode

Usage Guide This command is used to configure the line to accept both dial-in and dial-out. The DTR signal is always in the up status.

Configuration Examples The following example makes the line corresponding to the backup interface accept both dial-in and dial-out:

```
Ruijie(config)# line aux 0
Ruijie(config-line)# modem inout
```

Related Commands

Command	Description
modem dialin	Configures the line to accept dial-in only.

Platform Description N/A

Command History

Version	Description
N/A	N/A

peer default ip address

Use this command to specify the default IP address for remote dialup user.
Use the **no** form of this command to cancel the default IP address for the remote dial-in user.
peer default ip address { *ip-address* | **pool** [*pool-name-list*] }
no peer default ip address

Parameter Description

Parameter	Description
ip-address	Specifies a clear IP address for dial-in users. To prevent multiple dial-in users from using duplicate IP addresses, do not use this parameter in the legacy DDR to specify a clear IP address for dial-in user.
pool	If the pool-name-list is not used to specify the address pool at the end, the address pool specified in the global default address allocation policy will be used.
pool-name-list	Address pool name

Defaults The local default IP address pool specified in the global default address allocation policy is used to allocate IP address of the dial-in users.

Command Mode Interface configuration mode

Usage Guide This command specifies default IP addresses in PPP connections. If the remote user has no local address specified, the specified default IP address will be used.
In the following cases, this command overwrites the policy specified in the global default address allocation policy:

- Use **peer default ip address** *ip-address* to specify a clear IP address for the user
- Use **peer default ip address pool-name-list** to specify the local address pool to allocate IP address for the user

Configuration Examples The following example specifies the a clear IP address for the remote dial-in users of asynchronous interface 1:

```
Ruijie(config)# interface async 1
Ruijie(config-if)# peer default  ip address 1.1.1.2
```

Related Commands

Command	Description
ip address-pool	Sets the global default address policy.
ip dhcp-server	Specifies the DHCP server.
ip local pool	Configures the local address pool.

Platform Description N/A

Command History

Version	Description
N/A	N/A

pppoe enable

Use this command to enable the PPPoE on the Ethernet interface.
Use the **no** form of this command to close PPPoE.
pppoe enable
no pppoe enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults PPPoE is disabled.

Command Mode Interface configuration mode

Usage Guide This command is one of the necessary commands for PPPoE dialup, which is used to enable the PPPoE function of the interface.
Generally it is used when PPPoE is used for Ruijie's RGOS series devices.

Configuration Examples The following example enables the PPPoE on Ruijie's RGOS series Ethernet:

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if)# pppoe enable
```

Related Commands

Command	Description
pppoe-client	Enables the PPPoE DDR function.

Platform Description N/A

Command History

Version	Description
N/A	N/A

pppoe-client

Use this command to configure the PPPoE DDR function on the Ethernet interface.
Use the **no** form of this command to cancel the PPPoE DDR function.
pppoe-client dial-pool-number *number* **dial-on-demand**
no pppoe-client dial-pool-number *number* **dial-on-demand**

Parameter Description

Parameter	Description
number	Number of the dialer pool
dial-on-demand	PPPoE Client trigger mode
no-ddr	PPPoE Client perpetual online mode

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to bind the Ethernet interface to a dialer pool. The logical interface uses the specified dialer pool to establish the association between Ethernet interface and logical interface to implement DDR.
If there comes a message that match the simulation dialup rule but the line is not up yet, it stimulates the Ethernet interface for PPPoE dialup. If there is no data communication within the specified line idle period, the line will be disconnected.

Configuration Examples The following example binds Ethernet interface 1 to dialer pool 1 and enables the PPPoE DDR function:

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# pppoe-client dial-pool-number 1 dial-on-demand
```

Related Commands

Command	Description
pppoe enable	Enables the PPPoE function.

Platform Description N/A

Command History

Version	Description
N/A	N/A

script dialer

Use this command to associate the MODEM script to be executed in DDR dialup.
Use the **no** form of this command to cancel the association.
script dialer *script-name*
no script dialer

Parameter Description

Parameter	Description
script-name	Name of the script

Defaults The default script is used for dialup.

Command Mode Line configuration mode

Usage Guide This command is used to associate the script to be executed in the DDR dialup.


Caution

In the RGOS versions below V6.11, there is no script configured for dialup. So, it is necessary to use this command to specify the dialup script. In V6.11 or above, the RGOS has default dialup script, no additional configuration needed.

Configuration Examples The following example configures the script to be executed in the DDR dialup on the backup interface:

```
Ruijie(config)# line aux 0
Ruijie(config-line)# script dialer chat_dial
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

show ip pool

Use this command to show the local address pool in privileged EXEC mode.

show ip pool [*pool-name*]

Parameter Description

Parameter	Description
pool-name	Name of the local address pool

Command Mode Privileged EXEC mode

Configuration Examples The following following exampleshows the output of the command:

```
Ruijie# show ip local pool
Pool     Begin          End            Free InUse
star     1.1.1.3        1.1.1.10       8    0
```

The parameters are quite simple and therefore are not explained here.

Related Commands

Command	Description
ip address-pool	Defines the global default address allocation policy.
ip local pool	Defines the local address pool.

Platform Description N/A

Command History

Version	Description
N/A	N/A

show pppoe

Use this command to view the PPPoE status information.

show pppoe { **session** | **tunnel** | **ref**}

Parameter Description

Parameter	Description

session	Shows the session information.
ref	Shows the fast forwareding information.

Usage Guide The **session** and **tunnel** status information of this command is the same.

Configuration Examples The following example shows the output of the command.

```
Ruijie# show pppoe tunnel
pppoe tunnel state
state is TERMINATED ,my mac is 4E.54.38.00.00.01 , peer mac is 00.D0.F8.38.AA.20
Next timer fires after: 00:00:14
```

There are six statuses of PPPoE:

- SENT_IDLE Idle
- SENT_PADI PADI sent
- RECEIVED_PADO PADO received
- SENT_PADR PADR sent
- SESSION Enter the Session stage
- TERMINATED Session terminated

Next timer fires after: Indicate the time from now to the next status action

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

WAN-4G Commands

apply detect

Use this command to configure associated interface protocol status and the association of the 4G link with the dial stimulation rule. Use the **no** form of this command to restore the default setting.

apply detect {dial-list { *list_id* | l*ist_name* [**idle-timeout** *seconds*] } **| interface** *intf_name* { **bfd | track** *track_id* **| rssi-detect** *rssi-value* **interval** *check-interval* **ntimes** *check-times* **percent** *percent-value*}}

no apply detect { **dial-list | interface** *intf_name* { **bfd | track** *track_id* **| rssi-detect** *rssi-value* **interval** *check-interval* **ntimes** *check-times* **percent** *percent-value* }

Parameter Description

Parameter	Description
dial-list	Indicates the associated dial stimulation rule.
list_id	Indicates the ACL ID of dial stimulation.
l*ist_name*	Indicates the ACL name of dial stimulation.
seconds	Indicates idle timeout of the link. The default value is 120s.
intf_name	Indicates the name of the associated master interface.
bfd	Indicates the BFD status of the associated master interface.
track	Indicates the Track status of the associated master interface.
track_id	Indicates the Track ID of the associated master interface.
rssi-detect	Configures association of single 4G card status with RSSI detection.
track	Configures association of single 4G card status with Track.
bfd	Configures association of single 4G card status with BFD.
rssi-value	Specifies a threshold for signal strength. Detection starts when signal strength is below the threshold. The detection range is from -150 to -1 with dbm as the unit.
check-interval	Specifies the time range for continuous detection of signal strength. The time range is from 5 to 120 with second as the unit.
check-times	Specifies detection times within the time range. The range for detection times is from 1 to 30.
percent-value	Configures the percent of successful RSSI detection among all detection. The range is from 1 to 100.

Defaults By default, associated interface protocol status and the association of the 4G link with the dial stimulation rule are not configured.

Command Mode Interface configuration mode.

Usage Guide 1. This feature should be configured before enabling dial-on-demand, backup and anti-traffic-impact.

2. There are up to 8 protocols and dial stimulation rules combined. Only one dial stimulation rules can

be configured at most.
3. This command is only used to configure rule association. To enable dial-on-demand, backup and anti-traffic-impact, run corresponding commands after executing this one. For details, please refer to related description of these features.
4. A specified dial link is disconnected after no interesting packets are received within the idle-timeout period. If an interesting packet is received during the idle-timeout period, the period resets. The default idle-timeout is 120s and is not displayed.
5. If list ID or name is not created, all packets satisfy dial rules.

Configuration Examples

1. The following example configures association with BFD protocol of interface vlan 10 on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# apply detect interface vlan 10 bfd
```

2. The following example configured association with dial stimulation rule on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# apply detect dial-list 200
```

3. The following example configures association with dial stimulation rule and BFD protocol of interface vlan 10 on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# apply detect dial-list 200
Ruijie(config-if-Cellular0/0)# apply detect interface vlan 10 bfd
```

Related Commands

Command	Description
apply dial-on-demand	Configures dial-on-demand.
apply traffic-anti-impact	Configures anti-traffic-impact.

Platform Description

N/A

apply dial-on-demand

Use this command to configure dial-on-demand and the random delay access range. And use the **no** form of this command to restore the default setting.

apply dial-on-demand [**min-delay** *delay1* **max-delay** *delay2*]

no apply dial-on-demand

Parameter Description

Parameter	Description
min-delay *delay1*	Specifies minimum of the random delay access range. The range is from 1s to 300s. Not configuring this value means immediate access.

max-delay *delay2*	Specifies maximum of the random delay access range. The range is from 1s to 300s.

Defaults By default, this function is disabled.

Command Mode Interface configuration mode

Usage Guide The association with master interface protocol status must be configured for dial-on-demand.

Configuration Examples The following example configures dial-on-demand on the interface cellular 0/0 and sets the delay range to 10s-50s.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# apply detect interface vlan 10 bfd
Ruijie(config-if-Cellular0/0)# apply dial-on-demand min-delay 10 max-delay 50
```

Related Commands

Command	Description
apply detect	Configures association with the master interface.

Platform Description N/A

apply profile-auto-switch

Use this command to enable the master account every time when the master link is re-selected. Use the **no** form of this command to restore the default setting.

apply apply profile-auto-switch {**enable** | **disable**}

no apply apply profile-auto-switch

Parameter Description

Parameter	Description
enbale	Enables the master account when the master link is re-selected, when dual accounts are configured.
disable	Enables the most recently used account before the switch back to the master link, when dual accounts are configured.

Defaults By default, automatic switch is enabled.

Command Mode Interface configuration mode

Usage Guide Ensure the following conditions before running this command:

1. 4G link works as the backup link for other links.

2. Both master and slave accounts are configured.

Configuration Examples The following example configures the interface cellular 0/0 as the backup link for vlan10, configures both master and slave accounts and automatic switch.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# apply detect interface vlan 10 bfd
Ruijie(config-if-Cellular0/0)# apply dial-on-demand min-delay 10 max-delay 50
Ruijie(config-if-Cellular0/0)# profile create master apn aaaa username abc
password 0 123 track 10
Ruijie(config-if-Cellular0/0)# profile create slave apn bbbb username abc
password 0 123 track 20
Ruijie(config-if-Cellular0/0)# apply profile-auto-switch enable
```

Related Commands

Command	Description
profile creat	Configures dial accounts.

Platform Description N/A

apply traffic-anti-impact

Use this command to configure the anti-traffic-impact function. Use the **no** form of this command to restore the default setting.

apply traffic-anti-impact interface *intf_name* **list** {*list_id* | l*ist_name*}

no apply traffic-anti-impact

Parameter Description

Parameter	Description
intf_name	Interface name. Anti-traffic-impact works on the traffic flowing through this interface.
list_id	ACL ID for limiting traffic.
list_name	ACL name of traffic.

Defaults By default, this function is disabled.

Command Mode Interface configuration mode

Usage Guide Configure protocol state association of the primary interface to perform anti-traffic-impact.

Configuration Examples The following example configures anti-traffic-impact on the interface cellular 0/0 to block traffic of VLAN1 from impacting the network through the 4G interface. .

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# apply detect interface vlan 10 bfd
```

```
Ruijie(config-if-Cellular0/0)# apply traffic-anti-impact interface vlan 1
list 100
```

Related Commands	Command	Description
	apply detect	Configures association with the master interface.

Platform Description This command is only supported on the RSR820 series.

backup-valid-check

Use this command to configure the time and count of checking the availability query timer. Use the no form of this command to remove the configuration.

backup-valid-check valid-timer {***seconds***} **max-check-times** {***max-times***}

no backup-valid-check

Parameter Description	Parameter	Description
	seconds	The timeout range is from 10s to 6,000s. The default value is 30s.
	max-times	The range of detection times is from 3 times to 30 times. The default value is 3 times.

Defaults The default timeout value is 60s and the default detection time is 3 times.

Command Mode Interface configuration mode.

Usage Guide After association with Track is configured on an interface, if the Track status remains to be down, the corresponding 4G interface is still unavailable in this situation. In this case, this timer needs to be started to perform check. If it is within the time of set "seconds * max-times", the time is 60s * 3 = 180s (the default configuration is used as an example), the corresponding Track status is still down, and related actions are needed.

1. Parameters set in this command take effect only on Track detection. And effective times are counted after successful dial.
2. When the associated Track is down, the timer starts operation. If the associated Track is up, the timer is off.
3. In actual scenarios, when Track detection is enabled, the time parameter set in this command should be longer than that of Track detection, or repeated switches between interfaces are caused. For example, Track detection operates every 60s, then this command is recommend to be configured as:

backup-valid-check valid-timer 30 max-check-times 3

Configuration Examples The following example configures on the interface cellular 0/0 the time and count of checking the availability query timer.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
```

```
Ruijie(config-if-Cellular0/0)#backup-valid-check valid-timer 30
max-check-times 3
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

plmn pin-protection

Use this command to enable the PIN code protection function. Three modes can be chosen in this command: simpel/bind-router/strct-pin. Use the no form of the command to restore the default setting.
plmn pin-protection { simple | bind-router | strct-pin *hash-code* **}** *encryption-type pincode*
no plmn pin-protection

Parameter Description	Parameter	Description
	simple	Indicates simple PIN code protection mode. In this mode, if the PIN code is input, the SIM card will be locked. (To unlock the SIM card, input the PIN code again.)
	strict-pin	Indicates strictly encrypted PIN code protection mode. In this mode, the PIN code is replaced by the HASH string, which is an 8-digit random password. In this case, the SIM card is locked. (To unlock the SIM card, input the PIN code.)
	bind-router	Indicates the PIN code protection function of router binding mode. In this mode, the current PIN code is replaced after hashing using the router serial number, which is an 8-digit random password. In this case, the SIM card is locked. (To unlock the SIM card, input the PIN code.)
	pincode	Indicates the PIN code of the current SIM card, which contains 4 to 8 digits.
	encryption-type	Indicates the encryption type of the PIN code. “0” stands for plaintext while “7” for ciphertext.
	pincode	Indicates the PIN code of the current SIM card, which contains 4 to 8 digits.
	hash-code	Indicates the HASH string in the strictly encrypted PIN code protection mode. The string is supposed to include 8 to 16 digits.

Defaults By default, the PIN code protection mode is disabeld.

Command Mode Interface configuration mode

Usage Guide 1. When the encryption-type is 0, the password is in plaintext. When the encryption –type is 7, the password is in ciphertext.

2. The default PIN code is 1234. In the simple PIN code protection mode, run the **pin-modify** command to modify the PIN code.
3. For details about PIN code protection modes, please refer to *WAN-4G-SCG*.
4. When the PIN code protection function is enabled through CLI, enter the correct PIN code of the SIM card. If the PIN code is wrong. The SIM card will be locked. PUK unlocking is needed.
5. Busy carriers may cause failed execution of the command.
6. Run the **no plmn pin-protection** command to disable PIN code protection function. This command can be executed only when the PIN code protection command is executed.

Configuration Examples

The following example enables simple PIN code protection function on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# plmn pin-protection simple 0 1234
```

The following example enables strictly encrypted PIN code protection function on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# plmn pin-protection strict-pin 12345678 0 1234
```

The following example enables the PIN code protection function of router binding mode on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# plmn pin-protection bind-router 0 1234
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

plmn pin-modify

Use this command to modify the current PIN code after the simple PIN code protection function is enabled. After modifying, you need to save the configuration.

plmn pin-modify *pinnew*

Parameter Description

Parameter	Description
pinnew	Specifies new PIN code, which contains 4 to 8 digits.

Defaults

By default, this function is disabled.

Command Mode

Interface configuration mode

Usage Guide

1. This command can be performed only in the simple PIN code protection mode.

2. During configuration, there are man-machine interactions. Choose “Y” to save the modified configuration or the new PIN code is invalid.
3. The PIN code cannot be modified if the PIN code protection function of router binding mode or the strictly encrypted PIN code protection function is enabled.
4. PIN code modifying does not cause re-dialing of interfaces.
5. The command may fail due to a busy system.
6. There is not a **no** form of this command.

Configuration Examples The following example modifies the PIN code on the interface cellular 0/0..

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# plmn pin-protection simple 0 1234
Ruijie(config-if-Cellular0/0)# plmn pinb-modify 12345678
Proceed with modify pin code and write config? [N0] y
pin code modify success !
```

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

Platform Description N/A

plmn puk-unlock

Use this command to perform PUK unlocking and reset the PIN code. The SIM card will be locked when a wrong PIN code is used to enable PIN code protection. In this case, PUK unlocking is needed, and a new PIN code needs to be set for the SIM card. The SIM card will be damaged when the number of wrong PUK code attempts reaches 10. Before unlocking, you are recommended to first ask the operator about the PUK code corresponding to the SIM card. PUK unlocking can also be implemented through a mobile phone or other terminals.

plmn puk-unlock *pukcode pincode*

Parameter Description	**Parameter**	**Description**
	pukcode	Indicates the PUK code of the SIM card.
	pincode	Indicates the newly-set PIN code, which contains 4 to 8 digits.

Defaults By default, this feature is disabled.

Command Mode Interface configuration mode

Usage Guide 1. The SIM card will be locked when a wrong PIN code is used to enable PIN code protection. In this case, PUK unlocking is needed, and a new PIN code needs to be set for the SIM card. Use the PUK unlocking command with caution. The SIM card will be damaged when the number of wrong PUK code attempts reaches 10. Before unlocking, you are recommended to first ask the operator about

the PUK code corresponding to the SIM card.
2. The command may fail due to a busy system.
3. There is not a **no** form of this command.
4. After successful unlocking, if automatic dialing has been configured on the interface, automatic dialing starts on the interface. Network quality of operators and signal strength causes differences in dialing time, whose normal range is from 20s to 120s.

Configuration Examples The following example modifies the PIN code on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# plmn pin-protection simple 0 1234
Ruijie(config-if-Cellular0/0)# plmn puk-unlock 12345678 1234
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

plmn sent-username

Use this command to configure APN, user name and password. Use the no form of this command to remove the configuration.
plmn sent-username *uname-string* **password** { **0 | 7**} *pw-string* { *apn apn-string* }
no plmn sent-username

Parameter Description

Parameter	Description
uname-string	Specifies the user name, which contains less than 64 valid characters.
0 /7	Specifies plaintext or cyphertext.
pw-string	Specifies the password, which contains less than 52 valid characters.
apn-string	Specifies the APN distributed by the operation, which contains less than 40 valid characters.

Defaults By default, this function is disabled.

Command Mode Interface configuration mode

Usage Guide 1. A public network SIM card can access the network normally without configuring the APN. The APN can also be configured manually by referring to the public network access requirements of the operator's network.
2. The APN needs to be correctly configured for a dedicated line SIM card. If there is an APN configuration error, the SIM card may access a public network.
3. Any changes to the APN, username and password of the master account via this command trigger

another round of dialing.

Configuration Examples The following example configures the APN, user name and password on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# #plmn sent-username abc password 0 123 apn 111
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

plmn status

Use this command to configure RSSI detection on a 4G interface. Use the **no** form of this command to remove the configuration.

plmn status { **rssi-detect** *rssi-value* **interval** *check-interval* **ntimes** *check-times* **percent** *percent-value* | **track** *track-id* **| bfd** }

no plmn status

Parameter Description

Parameter	Description
rssi-detect	Configures a single 4G interface to associate with RSSI detection.
track	Configures a single 4G interface to associate with track.
bfd	Configures a single 4G interface to associate with BFD.
rssi-value	Specifies a threshold for signal strength. Detection starts when signal strength is below the threshold. The detection range is from -150 to -1 with dbm as the unit.
check-interval	Specifies the time range for continuous detection of signal strength. The time range is from 5 to 120 with second as the unit.
check-times	Specifies detection times within the time range. The range for detection times is from 1 to 30.
percent-value	Configures the percent of successful RSSI detection among all detection. The range is from 1 to 100.
track_id	Specifies the associated track ID.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is used to configure a 4G interface to associate with RSSI detection, track object or BFD status. But only one association at one time is possible.

Association with RSSI detection is configured:

```
interface cellular 0/0
plmn status rssi-detect -90 interval 20 ntimes 4 percent 50
```

After this command is run, there are four RSSI detections within 20s. If signal strength is below -90dbm in two (4 x 50%) or more out of the four detections, the corresponding link is disconnected.

Association with Track object is configured:
After successful dialing, if the Track status is up, it means the Track object is active, so the dial-up connection remains on the 4G interface. If the Track status changes to down, link of the 3G interface is disconnected.

Association with BFD status is configured:
After successful dialing, if the BFD status is up, the dial-up connection remains on the 4G interface. If the BFD status changes to down, link of the 4G interface is disconnected.

Configuration Examples

1. The following example configures RSSI detention on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)#plmn status rssi-detect -90 interval 15 ntimes 3 percent 100
```

2. The following example associates Track with the async1 interface.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# plmn status track 1
```

3. The following example associates BFD with the cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)#plmn status bfd
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

plmv vpdn-option

Use this command on the 4G interface to enable IMSI authentication. Use the **no** form of this command to restore the default setting.

plmn vpdn-option send-imsi

no plmn vpdn-option send-imsi

Parameter

Parameter	Description

Description	N/A	N/A

Defaults By default, this function is disabled.

Command Mode Interface configuration mode.

Usage Guide 1. When 4G VPDN is accessed, the IMSI number of the SIM card is required for authentication. Use this command to send the IMSI number to the remote router. After this feature is enabled, the IMSI number becomes part of the username to be sent to the authentication server. The complete username format is IMSI@#username.
2. Configure the username format of the authentication server to be IMSI@#username, too.

Configuration Examples The following example configures the username, password and APN for single card access on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# #plmn vpdn-option send-imsi
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

plmn telecom

Use this command to enable 3GPP dialing when EVDO or CDMA-1X private networks of China Telecom are accessed. Use the **no** form of this command to restore the default setting.
plmn telecom dial-3gpp
no plmn telecom dial-3gpp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, 3GPP2 is enabled.

Command Mode Interface configuration mode.

Usage Guide Usually, to access EVDO or CDMA-1X private networks of China Telecom, 3GPP2 dialing is enabled. But in some areas, to access the same private networks, 3GPP dialing needs to be enabled.

Configuration Examples The following example enables 3GPP dialing on the interface 2/0.

```
Ruijie #configure
```

```
Ruijie(config-if-Cellular 2/0)#plmn telecom dial-3gpp
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

profile create

Use this command to create the APN, username, password and backup for dialing on the 4G interface. Use the **no** form of this command to remove the configuration.

profile create { **master** | **slave** } [**apn** *apn-string*] **username** *uname-string* **password** { **0** | **7** } *pw-string* { **bfd** | **track** *track_id* }

no profile create { **master | slave** }

Parameter Description	Parameter	Description
	master	Indicates the master dialing configuration template.
	slave	Indicates the slave dialing configuration template.
	apn-string	Indicates the APN distributed by the operator.
	uname-string	Indicates the username.
	0/7	Selects plaintext or ciphertext.
	pw-string	Indicates the password.
	track_id	Indicates the associated Track ID.

Defaults By default, the function is disabled.

Command Mode Interface configuration mode.

Usage Guide

1: A public network SIM card can access the network normally without configuring the APN. The APN can also be configured manually by referring to the public network access requirements of the operator's network.
2: The APN needs to be correctly configured for a dedicated line SIM card. If there is an APN configuration error, the SIM card may access a public network.
3: Any changes to the APN, username and password of the master dialing configuration template via this command trigger another round of dialing. Changes to the parameters of the slave dialing configuration template do not trigger another round of dialing.
4: After the interface is associated with Track, if the Track status changes to down, the link is disconnected immediately and a new round of dialing is triggered. In this way, link is resumed efficiently.
5: After successful dialing, if the Track status is and continues to be down, the link is disconnected immediately and a new round of dialing is triggered. Run the **backup-valid-check** command to set the time range for continuous detection.
6: This command is used to configure backup of single 4G card and multiple access dialing function.

Configuration Examples

The following example configures the APN, username, password and Track on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# profile create master apn aaaa username abc
password 0 123 track 10
```

Related Commands

Command	Description
profile switch timer	Defines the timer for profile switch.
profile switch access-point	Defines the access for profile switch.

Platform Description

N/A

profile create master apn

Use this command to configure the APN on the 4G interface. Use the **no** form of this command to remove the configuration.
profile create master apn *apn-string*
no profile create master [apn]

Parameter Description

Parameter	Description
apn-string	Defines the APN distributed by the operator.

Defaults

By default, no APN is configured.

Command Mode

Interface configuration mode.

Usage Guide

1: A public network SIM card can access the network normally without configuring the APN. The APN can also be configured manually by referring to the public network access requirements of the operator's network.

2: The APN needs to be correctly configured for a dedicated line SIM card. If there is an APN configuration error, the SIM card may access a public network.

3: After the APN or PCO configuration is modified, validate the configuration by using any one of the following three methods:

Method 1: Execute **reset** on the interface to reset the interface.

```
Ruijie(config-if-Cellular0/0)# reset
```

Method 2: Execute **shutdown** on the interface, and then execute **no shutdown** after waiting for at least two seconds.

```
Ruijie(config-if-Cellular0/0)# shutdown
.....
Ruijie(config-if-Cellular0/0)# no shutdown
```

Method 3: Save the configuration and restart the host.

```
Ruijie #write
Ruijie #reload
Proceed with reload? [no]y
```

If the configuration under the 4G interface is modified by remotely logging in to the device through the 4G line, only method 1 or 2 can be used. Any of the three methods can be used if the configuration is not modified through the 4G line.

Configuration Examples

The following example configures APN on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)#profile create master apn gongan
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

profile create master track

Use this command to configure the ID of the Track object associated with the 4G interface status. Use the **no** form of this command to remove the setting.

profile create master track *track_id*

no profile create master [track]

Parameter Description	Parameter	Description
	track_id	Specifies the ID of the associated Track object.

Defaults By default, the ID of the Track object associated with the 4G interface status is not configured.

Command Mode Interface configuration mode

Usage Guide 1: After the interface is associated with Track, if the Track status changes to down, the link is disconnected immediately and a new round of dialing is triggered. In this way, link is resumed efficiently.
2: After successful dialing, if the Track status is and continues to be down, the link is disconnected immediately and a new round of dialing is triggered. Run the **backup-valid-check** command to set the time range for continuous detection.

Configuration Examples The following example configures the ID of the Track object associated with the 4G interface status on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)#profile create master track 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

profile create master username

Use this command to configure the specified user name/password. Use the **no** form of this command to restore the default setting.
profile create master username *uname* **password** { **0 | 7** } *pw*
no profile create master [username]

Parameter Description	Parameter	Description
	uname	Indicates the username.
	0/7	Selects plaintext or ciphertext.
	pw	Indicates the password.

Defaults By default, this function is disabled.

Command Mode Interface configuration mode.

Usage Guide After the APN or PCO configuration is modified, validate the configuration by using any one of the following three methods:

Method 1: Execute **reset** on the interface to reset the interface.

```
Ruijie(config-if-Cellular0/0)# reset
```

Method 2: Execute **shutdown** on the interface, and then execute **no shutdown** after waiting for at least two seconds.

```
Ruijie(config-if-Cellular0/0)# shutdown
.....
Ruijie(config-if-Cellular0/0)# no shutdown
```

Method 3: Save the configuration and restart the host.

```
Ruijie #write
Ruijie #reload
Proceed with reload? [no]y
```

If the configuration under the 4G interface is modified by remotely logging in to the device through the 4G line, only method 1 or 2 can be used. Any of the three methods can be used if the configuration is not modified through the 4G line.

Configuration Examples The following example configures PCO in the interface cellular 0/0.

```
Ruijie #configure
Ruijie (config)#interface cellular 0/0
Ruijie (config-if-Cellular0/0)#profile create master username aaa password 0
bbb
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

profile switch access-point

Use this command to switch the access point information.

profile switch access-point

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, this function is disabled.

Command Mode Interface configuration mode.

Usage Guide This command is used to back up dual access points of a single 4G card. After the command is executed, the current dialing connection gets broken. And the other dialing configuration template configured on the current interface is applied, so another round of dialing is triggered. In this way, switch between the master account and slave account is possible.

Configuration Examples The following example switches the access point information on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# profile switch access-point
```

Related Commands

Command	Description
profile switch timer	Defines the switch timer for dialing template.
profile creat	Defines the dialing template configuration.

Platform Description N/A

profile switch timer

Use this command to configure the switch timer on a 4G interface. Use the **no** form of this command to remove the configuration.

profile switch timer *seconds* **max-fail-times** *max-fail-times*

no backup-valid-check

Parameter Description

Parameter	Description
seconds	Specifies the timeout for the timer. The range is from 1s to 60s. The default value is 10s.
max-fail-times	Specifies the maximum detection times. The range is from 1 to 10. The default value is 3 times.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is supported when backup of single card and multiple hosts for the Track object is enabled.

The first status change of the Track objective does not cause switch between accounts. The timer is used to keep stability of the link. If the configured parameters are exceeded and the status of the Track object remains the same, switch between accounts is triggered.

For example, the command is configured as **profile switch timer 20 max-fail-times 3**. It means that 60s (20 x3) after the status change of the Track object, if the status of the Track object is still down,

then account switch is carried out.

Configuration Examples The following example configures the switch timer on the interface cellular 0/0.

```
Ruijie #configure
Ruijie(config)#interface cellular 0/0
Ruijie(config-if-Cellular0/0)# profile switch timer 20 max-fail-times 3
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

reset

Use this command to reset a 4G interface.

reset

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide After modifying configuration, such as APN, network type and user information, on an interface, run the **reset** command to make the modification come into effect on the interface.

Configuration Examples The following example resets the interface cellular 0/0.

```
Ruijie #configure
Ruijie (config)#interface cellular 0/0
Ruijie (config-if-Cellular0/0)#reset
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show cellular info

Use this command to display the current network access mode.

show cellular info [[**modem** | **network | radio | sim**] | [**interface** { **Cellular** *4g_interface*]

Parameter Description

Parameter	Description
modem	Displays information about hardware configuration and 4G modem.
network	Displays information about the 4G network.
radio	Displays information about signal of the 4G network.
sim	Displays information about the SIM card.
interface	Displays information about the specified 4G interface.
Cellular	Indicates the name of the 4G interface, which is the information source interface.
4g_interface	Specifies the number of the 4G interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays all the information about the 4G network.

```
host 192.168.12.91 255.255.255.240



-------Modem Information-------
 Slot           = 2
 Interface       = Cellular 0/0
 Software        = ZM8623_RSTV1.0.0B01
 Hardware        = y69B
 Imei           = 864424010005277
 Modem status    = Fully function(1)
 Modem name      = MF820S2

 ------Network Information------
 System mode     = LTE mode(17)
 System submode  = HSPA+ mode(9)
 Service state   = Effective service(2)
 Roam state      = Not roaming status(0)
 Service domain  = EPS service(4)
 Cell ID        = 134341892
 LAC           = 32796
 Band           = 38
 LTE subframe    = 0 , 0

 -----Modem Signal Strength-----
 RSRP           = -97dBm
```

```
--------Sim Information--------
Imsi           =
Phone          = Unknown
Sim status      = Effective(1)
Lock status     = PIN inactive(0)
PIN times       = 3
PUK times       = 10
```

Field Interpretation

Field	Interpretation
Modem information	Runs the **show cellular info modem** command to display information about hardware and the 4G module alone.
Slot	Indicates the number of the slot for the card.
Interface	Indicates the 4G information source interface.
Software	Indicates the software version of the 4G module.
Hardware	Indicates the hardware version of the 4G module.
IMEI	Indicates International Mobile Equipment Identity.
Modem name	Indicates the modem name.
Modem Status	Indicates the modem status.
Network Information	Runs the **show cellular info network** command to display information about the 4G network alone.
System mode	Indicates the current system mode.
System submode	Indicates the current system submode.
Service state	Service state includes following kinds: No service Restricted service Valid service Restricted regional service Power-saving and deep sleep state
Roam state	Roam state includes Non-Roaming state and Roaming state.
Service domain	Service domain includes following kinds: No service Only CS service Only PS service PS+CS service CS and PS not registered, searching
Cell ID	Indicates the cell ID for 4G access.
LAC	Indicates the location code.
Band	Indicates bandwidth.
LTE subframe	Indicates LTE subframe.
Modem Signal Strength	Run the **show cellular info radio** command to display information about 4G signal alone.
RSRP	Indicates the current signal strength.
Sim Information	Run the **show cellular info sim** command to display information

	about the SIM card alone.
IMSI	Indicates International Mobile Subscriber Identity.
Phone	Indicates the phone number of the SIM card.
Sim status	SIM card status includes following kinds: Invalid USIM card state or pin code locked Valid USIM card state USIM is invalid in case of CS USIM is invalid in case of PS USIM is invalid in case of either CS or PS USIM card is not existent
PIN times	Indicates PIN times of the SIM card.
PUK times	Indicates PUK times of the SIM card.
Signal strength	Indicates the current signal strength.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show plmn backup

Use this command to display information about link detection backup of the 4G card

show plmn backup

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Priviledged EXEC mode.

Usage Guide After this command is executed, information is displayed about interface, bound Track ID, Track status and availability detection.

Configuration Examples The following example displays status of link detection backup.

```
Ruijie#sh plmn backup
 plmn backup information:
 ----------------------
 Interface Cellular 0/0    :
 Backup type     : SINGLE_CARD_OTHER_HOST
 Detect type     : TRACK_DETECT
 Backup-Role     : SLAVE
 Detect intf     : VLAN 1
```

```
Current-Track-ID : 1 (Up)
Dial mode       : dial-on-demand mode
Dial delay max   : 0 secs
Dial delay min   : 0 secs
-------------------------------------------------
```

Field Interpretation

Field	Interpretation
Backup type	Backup (correlation) type: ● **SINGLE _CARD_OTHER_HOST**: Correlation backup with other interfaces or ACL is configured. ● **SINGLE_CARD_SINGLE_HOST**: Detection of single card and single host is configured. ● **SINGLE_CARD_DOUBLE_HOST**: Detection of single card and double host is configured.
Detect type	Correlated detection type: ● **RSSI-DETECT**: Indicates detection correlated with RSSI. ● **BFD-DETECT**: Indicates detection correlated with BFD. ● **TRACK-DETECT**: Indicates detection correlated with Track. ● **ACL-DETECT**: Indicates correlation with ACL.
Backup-Role	Detection role of the current interface: ● **MASTER**: It is the master interface. ● **SLAVE**: It is the slave interface. ● **MYSELF**: Single card status detection is configured on the interface.
Detect intf	Name of the interface for **SINGLE_CARD_OTHER_HOST** mode correlation.
Current-Track-ID	Indicates the correlated Track ID.
Dial mode	Dial mode of the current interface: ● **dial-on-demand mode:** It is dial-on-demand mode. ● **auto-dial mode:** It is automatic dial mode.
Dial delay max	Indicates the maximum dial delay.
Dial delay min	Indicates the minimum dial delay.

```
plmn backup information:
 ----------------------
 Interface Cellular 0/0:
 Backup type     : SINGLE_CARD_SINGLE_HOST
 Detect type     : TRACK_DETECT
 Backup-Role    : MYSELF
 Current-Track-ID: 1 (Up)

 Valid_Timer     : Running
 Valid-Times (60 Sec), Max-Check-Times (3 times)
 Current vaild fail times: 0
 Times before next valid check: 56 secs
```

```
Dial mode       : auto-dial mode
-----------------------------------------------------
```

Field Interpretation

Field	Interpretation
Backup type	Backup (correlation) type: ● **SINGLE _CARD_OTHER_HOST**: Correlation backup with other interfaces or ACL is configured. ● **SINGLE_CARD_SINGLE_HOST**: Detection of single card and single host is configured. ● **SINGLE_CARD_DOUBLE_HOST**: Detection of single card and double host is configured.
Detect type	Correlated detection type: ● **RSSI-DETECT**: Indicates detection correlated with RSSI. ● **BFD-DETECT**: Indicates detection correlated with BFD. ● **TRACK-DETECT**: Indicates detection correlated with Track. ● **ACL-DETECT**: Indicates correlation with ACL.
Backup-Role	Detection role of the current interface: ● **MASTER**: It is the master interface. ● **SLAVE**: It is the slave interface. ● **MYSELF**: Single card status detection is configured on the interface.
Current-Track-ID	Indicates the correlated Track ID.
Dial mode	Dial mode of the current interface: ● **dial-on-demand mode:** It is dial-on-demand mode. ● **auto-dial mode:** It is automatic dial mode.
Dial delay max	Indicates the maximum dial delay.
Dial delay min	Indicates the minimum dial delay.
Valid_Timer	When detection is correlated with Track or BFD, availability detection monitors if the Track object or the BFD status remains down within the configured period. ● Running: It is launching. ● Stopped: It does not start.
Valid-Times **Max-Check-Times** **Current vaild fail times** **Times before next valid check**	Parameters detected by correlation detection availability: **Valid-Times**: Indicates timer for availability detection. **Max-Check-Times:** Indicates check times. **Current vaild fail times**: Indicates times of failed availability detection. **Times before next valid check:** Indicates the time left before the next detection.

```
Ruijie(config-if-Cellular 0/0)#sh plmn backup
 plmn backup information:
 ----------------------
 Interface Cellular 0/0:
 Backup type     : SINGLE_CARD_DOUBLE_HOST
```

```
Detect type     : TRACK_DETECT
Profile-Role   : MASTER
Current-Track-ID: 1 (Up)
Current Access Point: Apn(4gnet), Username(aaa)
Switch-Timer   : Stopped
Delay-Times (10 Sec), Max-Fail-Times (3 times)

Valid_Timer     : Stopped
Valid-Times (60 Sec), Max-Check-Times (3 times)

Dial mode       : auto-dial mode
-----------------------------------------------------
```

Field Interpretation

Field	Interpretation
Backup type	Backup (correlation) type: ■ **SINGLE _CARD_OTHER_HOST**: Correlation backup with other interfaces or ACL is configured. ■ **SINGLE_CARD_SINGLE_HOST**: Detection of single card and single host is configured. ■ **SINGLE_CARD_DOUBLE_HOST**: Detection of single card and double host is configured.
Detect type	Correlated detection type: ■ **RSSI-DETECT**: Indicates detection correlated with RSSI. ■ **BFD-DETECT**: Indicates detection correlated with BFD. ■ **TRACK-DETECT**: Indicates detection correlated with Track. ■ **ACL-DETECT**: Indicates correlation with ACL.
Profile-Role	■ **MASTER**: It is the master interface. ■ **SLAVE**: It is the slave interface.
Current-Track-ID	Indicates the correlated Track ID.
Dial mode	Dial mode of the current interface: ■ **dial-on-demand mode:** It is dial-on-demand mode. ■ **auto-dial mode:** It is automatic dial mode.
Dial delay max	Indicates the maximum dial delay.
Dial delay min	Indicates the minimum dial delay.
Valid_Timer	When detection is correlated with Track or BFD, availability detection monitors if the Track object or the BFD status remains down within the configured period. ■ Running: It is launching. ■ Stopped: It does not start.
Valid-Times **Max-Check-Times** **Current vaild fail times**	Parameters detected by correlation detection availability: **Valid-Times**: Indicates timer for availability detection. **Max-Check-Times:** Indicates check times. **Current vaild fail times**: Indicates times of failed availability detection.

Times before next valid check	**Times before next valid check:** Indicates the time left before the next detection.
Profile-Role	■ **MASTER**: It is the master interface. ■ **SLAVE**: It is the slave interface.
Current Access Point	Indicates information about the current access point, such as information about APN and username.
Switch-Timer	Indicates the status of switch timer, when the Track object is detected to be down. ● Running: It is launching. ● Stopped: It does not start.
Delay-Times	Indicates switch delay.
Max-Fail-Times	Indicates needed detection times.
Current Fail times **Times before next Detecting**	**Current Fail times**: Indicates the times of the Track object to remain down. **Times before next Detecting**: Indicates the time left before the next detection.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Reliability Configuration Commands

1. RLDP Commands
2. MSTP Commands
3. LLDP Commands
4. VRRP Commands
5. Hot-Plugging/ Unplugging Commands
6. Multi-link Load Balance Commands
7. RNS&Track Commands

RLDP Command

debug rldp

Use this command to turn on the RLDP service debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug rldp [**packet** | **event** | **error**]

undebug rldp [**packet** | **event** | **error**]

Parameter Description

Parameter	Description
packet	Turns on the incoming/outgoing RLDP packet debugging switch.
event	Turns on the event debugging switch.
error	Turns on the error debugging switch.

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.

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.

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.

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.

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 demonstrates 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.

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.

show rldp

Use this command to show 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 N/A.

Description

MSTP Commands

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

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

Parameter	Description

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

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

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

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

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

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 Interface configuration mode.

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

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

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

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

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

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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

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

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

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

spanning-tree mst configuration

Use this command to enter the MST configuration mode in the global configuration mode and

configure the MSTP region. Use the **no** form of the command to restore the default setting.

spanning-tree mst configuration

no spanning-tree mst configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command 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 configure MSTP Region parameters:

Configuration Examples This example enters the MST configuration mode.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan  3, 5-10
Ruijie(config-mst)# name region 1
Ruijie(config-mst)# revision  1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    : region1
Revision : 1Instance  Vlans Mapped
----------  --------------------
0       1-2,4,11-4094
1       3,5-10
---------------------------------
Ruijie(config-mst)# exit
Ruijie(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the MST region configuration.
instance *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

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 Commands

Command	Description
show spanning-tree mst	Displays the MSTP information of an interface.
spanning-tree mst port-priority	Configures the priority of an interface.
spanning-tree mst priority	Configures the priority of an instance.

Platform Description

N/A

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

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

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

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

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

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

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

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

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

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

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

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-coun*t	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

LLDP Commands

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

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

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

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

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

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 The following example sets LLDP packet encapsulation format to

Examples

```
SNAP.Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if)#lldp encapsulation snap
```

Related Commands

Command	Description
show lldp status	Displays LLDP status information.

Platform Description N/A

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 Description N/A

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

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

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** *id* **| interface** *interface-name* **| static** }	Displays the LLDP Civic Address information.

Platform Description N/A

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

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

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

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

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

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 Description	Parameter	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

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

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

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

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 Description

Parameter	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

{ 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

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

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  : iiiiiiiii
Ports     : Gi1/0/3
```

```
--------------------------
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

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

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

show lldp statistics

The following example displays 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

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

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

VRRP Commands

debug vrrp

Use this command to turn on the VRRP error prompt, VRRP event, VRRP message and status debug switches.
Use the **no** form of this command to turn off the switches.
debug vrrp
no debug vrrp

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the debug switches are turned off.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows how to turn on the VRRP debug switch:

```
Ruijie# debug vrrp
Ruijie#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Master -> Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 1 state Backup -> Master
Ruijie#
```

Related Commands

Command	Description
Ruijie# **debug vrrp errors**	Turns on the VRRP error prompt debugging switch.
Ruijie# **debug vrrp events**	Turns on the VRRP event debugging switch.
Ruijie# **debug vrrp state**	Turns on the VRRP state debugging switch.

Platform Description N/A

Command

Version	Description

History	N/A	N/A

debug vrrp errors

Use this command to turn on the VRRP error prompt debug switch.

Use the **no** form of this command to turn off the switch

debug vrrp errors

no debug vrrp errors

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the VRRP error debug switch is turned off.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows how to turn on the VRRP error debug switch.

```
Ruijie# debug vrrp errors
Ruijie#
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

debug vrrp events

Use this command to turn on the VRRP event debug switch.

Use the **no** form of this command to turn off the switch.

debug vrrp events

no debug vrrp events

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the VRRP event debug switch is turned off.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows how to turn on the VRRP event debug switch.

```
Ruijie# debug vrrp events
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

debug vrrp packets

Use this command to turn on the VRRP packet debug switch.

Use the **no** form of this command to turn off the switch.

debug vrrp packets

no debug vrrp packets

Parameter Description

Parameter	Description

N/A	N/A

Defaults By default, the VRRP packet debug switch is turned off.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example shows how to turn on the VRRP packet debug switch, where the checksum of the packets of VRRP group 1 is displayed:

```
Ruijie# debug vrrp packets
Ruijie#
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
```

The following example shows how to turn on the VRRP packet debug switch, where the source IP address of the VRRP group 1 packets and the priority of VRRP group 1 are displayed:

```
Ruijie# debug vrrp packets
Ruijie#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

debug vrrp state

Use this command to turn on the VRRP status debug switch.
Use the **no** form of this command to turn off the switch.
debug vrrp state
no debug vrrp state

Parameter Description

Parameter	Description

N/A	N/A

Defaults By default, the VRRP debug switch is turned off.

Command Mode Privilege EXEC mode

Usage Guide N/A

Configuration Examples The following example shows how to turn on the VRRP status debug switch:

```
Ruijie# debug vrrp state
Ruijie#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Backup -> Master
Ruijie# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/0
Ruijie (config-if)#no shutdown
Ruijie(config-if)# end
Ruijie#
%VRRP-6-STATECHANGE: FastEthernet 0/0 Grp 2 state Master -> Init
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

show vrrp

Use this command to show the VRRP information.

show vrrp [**brief** | *group*]

Parameter Description

Parameter	Description
brief	(Optional) Shows 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 shows 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 shows 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 sets the IP address for the virtual device.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

show vrrp interface

Use this command to show 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) Shows 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 shows 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 sets the IP address for the virtual device.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

show vrrp packets statistics

Use this command to show 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 shows the statistics of VRRP packets transmitting on all interfaces:

```
Ruijie#show vrrp packet statistics

Total
  InReceives: 1000 packets, InOctets: 250, InErrors: 50
  OutTransmits: 900, OutOctets: 230
VLAN 1
  InReceives: 300 packets, InOctets: 100, InErrors: 6
  OutTransmits: 275, OutOctets: 75
VLAN 2
  InReceives: 500 packets, InOctets: 150, InErrors: 24
  OutTransmits: 450, OutOctets: 125
```

The example below shows the statistics of VRRP packets on the interface in VLAN2:

```
Ruijie#show vrrp packet statistics vlan 2

VLAN 2
  InReceives: 500 packets, InOctets: 150, InErrors: 24
  OutTransmits: 450, OutOctets: 125
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
10.4(3)	New command

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 the 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.


Caution 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
Ruijie(config-if)# vrrp *group* ipv6 *ipaddress*	Enables VRRP and configures an IPv6 address

	for the virtual router.

Platform Description N/A

vrrp authentication

Use this command to enable VRRP authentication.
Use the **no** form of this command to disable the 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 By default, the VRRP function is not enabled on the interface. 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 is only used to prevent/indicate 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
Ruijie(config-if)# **vrrp** *group ip ipaddress* [**secondary**]	Enables the VRRP function and sets the IP address for the virtual device.

Platform Description N/A

Command History

Version	Description
N/A	N/A

vrrp delay

Use this command to set the reload latency of the VRRP group on the interface. There are two types of reload latency: latency when the interface is up and latency when the system reloads. These two types can be configured together or separately.

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 By default, the VRRP reload delay function is not enabled on the interface. The default value ranges of the two parameters are both from 0 to 60.

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 not be reloaded immediately after the system reloads or the interface is up. If the interface receives VRRP packets during the latency, the latency is canceled and the VRRP protocol is enabled immediately. If this command is used for a network interface, it takes effect for IPv4 VRRP and IPv6 VRRP.

Configuration Examples The following example sets the VRRP reload latency on E0 to 10s. When E0 is up, VRRP group 1 shall be reloaded in 10s.

```
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
Ruijie(config-if)# **vrrp** *group ipaddress* [**secondary**]	Enables the IPv4 VRRP function and sets the IP address for the virtual device.
Ruijie(config-if)# **vrrp** *group* **ipv6** *ipv6-address*	Enables the IPv6 VRRP function and sets the IPV6 address for the virtual device.

Platform Description

Command History	Version	Description
	N/A	N/A

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 By default, the VRRP function is not enabled on the interface. 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 ipaddress* [**secondary**]	Enables the IPv4 VRRP function and sets the IP address for the virtual device.
	Ruijie(config-if)# **vrrp** *group* **ipv6** *ipv6-address*	Enables the IPv6 VRRP function and sets the IPV6 address for the virtual device.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

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 disable the VRRP function and remove the setting of virtual IP address.
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 VRRP 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]	Shows the VRRP configuration.

Platform Description N/A

Command	Version	Description

History	N/A	N/A

vrrp ipv6

Use this command to enable IPv6 VRRP on the interface and specify the related virtual IPv6 address. Use the **no** form of this command to disable the IPv6 VRRP function and remove the setting of virtual IPv6 address.

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 IPv6 VRRP 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**]	Shows the IPv6 VRRP configuration.

Platform Description Supported on all platforms.

vrrp preempt

Use this command to set the preemption mode of the VRRP group.
Use the **no** form of this command to disable the VRRP preemption function.
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 0s.

Defaults By default, the VRRP function is not enabled on the interface. 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 is insignificant, because that VRRP group has the highest priority and thereby automatically becomes the master device in the VRRP group.

Configuration Examples In the example below, once the VRRP group 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 s:

```
vrrp 1 preempt delay 15
vrrp 1 priority 200
```

Related Commands

Command	Description
Ruijie(config-if)# **vrrp** *group ipaddress* [**secondary**]	Enables the IPv4 VRRP function and sets the IP address for the virtual device.
Ruijie(config-if)# **vrrp** *group* **ipv6** *ipv6-address*	Enables the IPv6 VRRP function and sets the IPV6 address for the virtual device.
Ruijie config-if # **vrrp** *group* **priority** *level*	Sets the IPv4 VRRP group priority.
Ruijie(config-if)# **vrrp ipv6** *group* **priority** *level*	Sets the IPv64 VRRP group priority.

Platform Description N/A

Command

Version	Description

History	N/A	N/A

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 By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the priority of VRRP group 1 as 254:

```
vrrp 1 priority 254
```

Related Commands

Command	Description
Ruijie(config-if)# **vrrp** *group ipaddress* [**secondary**]	Enables the IPv4 VRRP function and sets the IP address for the virtual device.
Ruijie(config-if)# **vrrp** *group* **ipv6** *ipv6-address*	Enables the IPv6 VRRP function and sets the IPV6 address for the virtual device.

Platform Description N/A

Command History

Version	Description
N/A	N/A

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 *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
no vrrp *group* **timers advertise**

Parameter Description

Parameter	Description
group	VRRP group number
advertise-interval	Advertisement interval (in seconds)
csec *centisecond-interval*	The period for which the master router in the backup group sends VRRP packets, ranging from 50 to 99 milliseconds. There is no default value. It is valid only for VRRPv3. If VRRPv2 is configured with this command, the interval is one second by default.

Defaults

By default, the VRRP function is not enabled on the interface. Once the VRRP function is enabled, the default advertisement interval of the master device is 1 second.

Command Mode

Interface configuration mode

Usage Guide

If the current device becomes the master device in the VRRP group, it will indicate its VRRP status, priority and other information by sending the VRRP advertisement in the set interval.

Configuration Examples

The following example sets the IPv4 VRRP advertisement interval as 4 seconds.

```
vrrp 1 timers advertise 4
```

The following example sets the IPv6 VRRP advertisement interval as 4 seconds.

```
vrrp ipv6 1 timers advertise 4
```

The following example sets the IPv4 VRRP advertisement interval as 50 milliseconds.

```
vrrp 1 timers advertise csec 50
```

The following example sets the IPv6 VRRP advertisement interval as 50 milliseconds.

```
vrrp ipv6 1 timers advertise csec 50
```

Related Commands

Command	Description
Ruijie(config-if)# **vrrp** *group ipaddress* [**secondary**]	Enables the IPv4 VRRP function and sets the IP address for the virtual device.
Ruijie(config-if)# **vrrp** *group* **ipv6** *ipv6-address*	Enables the IPv6 VRRP function and sets the IPV6 address for the virtual device.
Ruijie config-if # **vrrp group timers learn**	Enables the IPv4 timer learning function.
Ruijie(config-if)# **vrrp ipv6** *group* **timers learn**	Enables the IPv6 timer learning function.

Platform Description

N/A

Command History

Version	Description
N/A	N/A

vrrp timers learn

Use this command to enable the timer learning function.
Use the **no** form of this command to disable the function.
vrrp *group* **timers learn**
no vrrp *group* **timers learn**

Parameter Description

Parameter	Description
group	VRRP group number

Defaults By default, the VRRP function is not enabled on the interface. 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 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

Command History

Version	Description
N/A	N/A

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 addrss via BFD. Use the **no** form of this command to disable this function.

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.
ipv6-global-addres	IPv6 global unicast address
ipv6-linklocal-addree	IPv6 link local 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	Timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1s.
retry-value	Number of reattempts before inaccessibility is confirmed. If no response is received after the number of reattempts reaches the value of *retry-value*, the inaccessibility is confirmed. The default value is 1.
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 By default, the VRRP function is not enabled on the interface. Even if the VRRP function is enabled, no interface or ip address (IPv4 or IPv6) is specified.

Command Mode

Usage Guide This command can be used to monitor the outlet links. Note that layer-3 routable logical interfaces can be monitored (such as Routed Port, SVI, Loopback and Tunnel).

If the host is to be monitored, for IPv4 virtual routers, specify the IPv4 address of the host; for IPv6 virtual routers, specify the IPv6 address of the host.

If the host address to be monitored is the local link address, a network interface must be specified.

If a VRRP group owns the actual IP address of an Ethernet interface, the priority of that group is 255

and the IP address or interface cannot be monitored.

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 shows how to set 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 IPv4 VRRP function and sets the IP address for the virtual device.
Ruijie(config-if)# **vrrp** *group* **ipv6** *ipv6-address*	Enables the IPv6 VRRP function and sets the IPV6 address for the virtual device.
Ruijie config-if # **vrrp** *group* **priority** *level*	Sets the IPv4 VRRP group priority.
Ruijie(config-if)# **vrrp ipv6** *group* **priority** *level*	Sets the IPv64 VRRP group priority.

Platform Description

N/A

Command History

Version	Description
RGOS 10.4	In RGOS 10.4 and higher, **vrrp track** can be followed by an IPv6 address.

vrrp version

Use this command to configure the version of sending the IPv4 VRRP multicast packets. For the IPv4 VRRP, there are two version: 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 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* [**secondary**]	Enables the VRRP function and set the IP 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

vrrp help

Use this command to show the typical VRRP configuration information.

vrrp help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration Examples

- Chinese interface

```
Ruijie#vrrp help

------------------------------------ 案例菜单 ------------------------------------
1、VRRP单备份组配置案例
2、使用VRRP监视接口配置案例
3、VRRP多备份组配置案例

按Esc键退出
----------------------------------------------------------------------------------
请选择您要查看的案例编号：1

------------------------------------ 配置需求 ------------------------------------
在SwitchA与SwitchB上部署VRRP备份组来为内部网段192.168.201.0/24提供VRRP服务，
SwitchA作为活动路由设备提供网关功能，当SwitchA由于关机或者出现故障而不可到达时，
SwitchB将替代它来提供网关(192.168.201.1)的功能。

------------------------------------ 配置步骤 ------------------------------------
1）配置SwitchA
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.217 255.255.255.0
//配置路由设备与内部网段相连的Gi0/1口的IP地址为192.168.201.217

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 priority 120
//设置IPv4 VRRP备份组1的优先级为120（默认值为100，数值越大，优先级越高）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//设置发送路由器公告的时间间隔为3s（默认值为1s）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.1

2）配置SwitchB
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.213 255.255.255.0
//配置路由设备与内部网段相连的Gi0/1口的IP地址为192.168.201.213

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//设置发送路由器公告的时间间隔为3s（默认值为1s）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.1
----------------------------------------------------------------------------------

Ruijie#
```

```
Ruijie#vrrp help

------------------------------------ 案例菜单 ------------------------------------
1、VRRP单备份组配置案例
2、使用VRRP监视接口配置案例
3、VRRP多备份组配置案例

按Esc键退出
----------------------------------------------------------------------------------
请选择您要查看的案例编号：2

------------------------------------ 配置需求 ------------------------------------
在SwitchA与SwitchB上部署VRRP备份组来为内部网段192.168.201.0/24提供VRRP服务，如果
SwitchA在作为Master路由设备状态下发现与广域网的接口Gi0/24不可用，将降低其VRRP备
份组优先级，SwitchB就会成为Master路由设备直到Gi0/24恢复可用，再次转换Master角色

------------------------------------ 配置步骤 ------------------------------------
1）配置SwitchA
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.217 255.255.255.0
//配置路由设备与内部网段相连的Gi0/1口的IP地址为192.168.201.217

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 priority 120
//设置IPv4 VRRP备份组1的优先级为120（默认值为100，数值越大，优先级越高）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//设置发送路由器公告的时间间隔为3s（默认值为1s）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.1
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 track gigabitEthernet 0/24 30
//设置IPv4 VRRP备份组监视的接口为Gi0/24，如果该接口IPv4协议状态是DOWN，把VRRP组1
//的优先级降低30

2）配置SwitchB
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.213 255.255.255.0
//配置路由设备与内部网段相连的Gi0/1口的IP地址为192.168.201.213

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//设置发送路由器公告的时间间隔为3s（默认值为1s）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.1
----------------------------------------------------------------------------------

Ruijie#
```

```
Ruijie#vrrp help

------------------------------------ 案例菜单 ------------------------------------
1、VRRP单备份组配置案例
2、使用VRRP监视接口配置案例
3、VRRP多备份组配置案例

按Esc键退出
--------------------------------------------------------------------------------
请选择您要查看的案例编号：3

------------------------------------ 配置需求 ------------------------------------
在SwitchA与SwitchB上部署VRRP备份组来为内部网段192.168.201.0/24提供VRRP服务，用户
工作站的网关指向不同备份组的虚拟IP地址，配置SwitchA和SwitchB使得它们在不同备份组
中实现负载均衡并通过互相备份来提供更稳定可靠的网络服务。

------------------------------------ 配置步骤 ------------------------------------
1）配置SwitchA
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.217 255.255.255.0
//配置路由设备与内部网段相连的Gi0/1口的IP地址为192.168.201.217

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//设置发送路由器公告的时间间隔为3s（默认值为1s）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.1
Ruijie(config-GigabitEthernet 0/1)#vrrp 2 priority 120
//设置IPv4 VRRP备份组2的优先级为120（默认值为100，数值越大，优先级越高）
Ruijie(config-GigabitEthernet 0/1)#vrrp 2 ip 192.168.201.2
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.2

2）配置SwitchB
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.213 255.255.255.0
//配置路由设备与内部网段相连的Gi0/1口的IP地址为192.168.201.213

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//设置发送路由器公告的时间间隔为3s（默认值为1s）
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.1
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 priority 120
//设置IPv4 VRRP备份组1的优先级为120（默认值为100，数值越大，优先级越高）
Ruijie(config-GigabitEthernet 0/1)#vrrp 2 ip 192.168.201.2
//启用IPv4 VRRP备份功能，对应网关ip为192.168.201.2
--------------------------------------------------------------------------------

Ruijie#
```

- English interface

```
Ruijie#vrrp help

---------------------------- Configuration Examples -----------------------------
1. Configuration example of VRRP single-backup group
2. Configuration example of using the VRRP monitoring interface
3. Configuration example of VRRP multi-backup group

Press "Esc" to exit
--------------------------------------------------------------------------------
Please choose the number you want to view: 1

------------------------- Configuration Requirements --------------------------
Deploy the VRRP backup group on the SwitchA and SwitchB to provide the VRRP
service for the inner network segment 192.168.201.0/24.The SwitchA serves as an
active routing device to provide the gateway function.On condition that the
SwitchA is unreachable due to the failure or shutting down, the SwitchB will
substitute it to provide the gateway(192.168.201.1) funciton.
----------------------------- Configuration Steps  -----------------------------
1) SwitchA Configuration
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.217 255.255.255.0
//Set the IP address of the interface Gi0/1 connecting the routing device with
//the intranet segment as 192.168.201.217
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 priority 120
//Set the priority of the IPv4 VRRP backup group1 as 120 (default:100, the
//greater the value, the higher priority is)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//Set the interval of sending VRRP advertisements as 3s (default: 1s)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.1

2) SwitchB Configuration
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.213 255.255.255.0
//Set the IP address of interface Gi0/1 connecting the routing device with the
//intranet segment as 192.168.201.213

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//Set the interval of sending VRRP advertisements as 3s (default: 1s)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.1
--------------------------------------------------------------------------------

Ruijie#
```

```
Ruijie#vrrp help

---------------------------- Configuration Examples -----------------------------
1. Configuration example of VRRP single-backup group
2. Configuration example of using the VRRP monitoring interface
3. Configuration example of VRRP multi-backup group

Press the Esc to exit
--------------------------------------------------------------------------------
Please choose the number you want to view: 2

------------------------- Configuration Requirements --------------------------
Deploy the VRRP backup group on the SwitchA and SwitchB to provide the VRRP
service for the intranet segment 192.168.201.0/24. If the interface Gi0/24
connecting with WLAN is unusable upon the SwitchA acting as the Master routing
device, the VRRP backup group priority of the SwitchA will be lowered ,and the
SwitchB will be the Master routing device untill the Gi0/24 is available, then
switch the Master role again.

------------------------------ Configuration Steps  ------------------------------
1) SwitchA Configuration
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.217 255.255.255.0
//Set the IP address of the interface Gi0/1 connecting the routing device with
//the intranet segment as 192.168.201.217

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 priority 120
//Set the priority of the IPv4 VRRP backup group1 as 120 (default:100, the
//greater the value, the higher priority is)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//Set the interval of sending VRRP advertisements as 3s (default: 1s)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.1
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 track gigabitEthernet 0/24 30
//Set the interface monitored by the IPv4 VRRP backup group as Gi0/24, if IPv4
//protocol state of the interface is down, lower the priority of VRRP group 1
//by 30


2) SwitchB Configuration
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.213 255.255.255.0
//Set the IP address of the interface Gi0/1 connecting the routing device with
//the intranet segment as 192.168.201.213

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//Set the interval of sending VRRP advertisements as 3s (default: 1s)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.1
--------------------------------------------------------------------------------

Ruijie#
```

```
Ruijie#vrrp help

---------------------------- Configuration Examples -----------------------------
1. Configuration example of VRRP single-backup group
2. Configuration example of using the VRRP monitoring interface
3. Configuration example of VRRP multi-backup group

Press "Esc" to exit
--------------------------------------------------------------------------------
Please choose the number you want to view: 3

------------------------- Configuration Requirements --------------------------
Deploy the VRRP backup group on the SwitchA and SwitchB to provide the VRRP
service for the intranet segment 192.168.201.0/24.
The gateway of user stations points to the virtual IP address of different
backup group.
Configure the SwitchA and SwitchB, so as to implement the load balancing in
different backup group and provide the more reliable and stable service through
the mutual backup
----------------------------- Configuration Steps  -----------------------------
1) SwitchA Configuration
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.217 255.255.255.0
//Set the IP address of the interface Gi0/1 connecting the routing device with
//the intranet segment as 192.168.201.217

Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//Set the interval of sending VRRP advertisements as 3s (default: 1s)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.1
Ruijie(config-GigabitEthernet 0/1)#vrrp 2 priority 120
//Set the priority of the IPv4 VRRP backup group2 as 120 (default:100, the
//greater the value, the higher priority is)
Ruijie(config-GigabitEthernet 0/1)#vrrp 2 ip 192.168.201.2
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.2


2) SwitchB Configuration
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-GigabitEthernet 0/1)#no switchport
Ruijie(config-GigabitEthernet 0/1)#ip address 192.168.201.213 255.255.255.0
//Set the IP address of the interface Gi0/1 connecting the routing device with
//the intranet segment as 192.168.201.213
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 timers advertise 3
//Set the interval of sending VRRP advertisements as 3s (default: 1s)
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 ip 192.168.201.1
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.1
Ruijie(config-GigabitEthernet 0/1)#vrrp 1 priority 120
//Set the priority of the IPv4 VRRP backup group1 as 120 (default:100, the
//greater the value, the higher priority is)
Ruijie(config-GigabitEthernet 0/1)#vrrp 2 ip 192.168.201.2
//Enable the IPv4 VRRP backup function and set the gateway 192.168.201.2
--------------------------------------------------------------------------------

Ruijie#
```

Note

You can switch the interface language between Chinese and English by running **language {Chinese|English}** in privileged EXEC mode.

Related Commands

Command	Description
view vrrp	Shows the main VRRP status information.

Platform This command is supported on layer-3 switches but not on routers.

Description

Command History	Version	Description
	10.4(3)	New command

vrrp *group* help

Use this command to show command instances that start with **vrrp** *group* in interface configuration mode.

vrrp *group* **help**

Parameter Description	Parameter	Description
	group	VRRP group number of the virtual device

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples

- Chinese interface

```
Ruijie(config-VLAN 1)#vrrp 1 help

命令举例：
------------------------------------------------------------------------------
>vrrp 1 ip 192.168.217.100

启用VRRP备份组1，设置该组的Primary IP地址为192.168.217.100；
1：备份组号（1-255）；        192.168.217.100：IP地址；
------------------------------------------------------------------------------
>vrrp 1 track gigabitEthernet 0/24 30

设置VRRP备份组监视的接口，端口只允许是三层可路由的逻辑接口。
1：备份组号（1-255）；        gigabitEthernet 0/24：端口0/24；
30：端口优先级变化值（默认值：10）
------------------------------------------------------------------------------
>vrrp 1 priority 120

设置VRRP备份组的优先级为120，数值越大则优先级越高；
1：  备份组号（1-255）；       120：优先级（默认值：100）
------------------------------------------------------------------------------
>vrrp 1 timers advertise 3

设置IPv4主路由设备VRRP通告间隔为3s
1：备份组号（1-255）；        3：VRRP通告发送间隔（默认值：1）
------------------------------------------------------------------------------
>vrrp 1 track 192.168.217.1 interval 10

设置IPv4 VRRP备份组监视的IP地址；
192.168.217.1：监视的IP地址；   10：探测该目标地址是否可达的间隔时间（默认值：3）
------------------------------------------------------------------------------
```

- English interface

```
Ruijie(config-if)#vrrp 1 help

Examples:
------------------------------------------------------------------------------
>vrrp 1 ip 192.168.217.100

Enable the VRRP backup group 1 and set the primary IP address 192.168.217.100;
1: backup group number (1-255) ;        192.168.217.100: IP address;
------------------------------------------------------------------------------
>vrrp 1 track gigabitEthernet 0/24 30

Configure the interface monitored by VRRP backup group. This interface can only
be a layer-3 routable logical interface.
1: backup group number (1-255):       gigabitEthernet 0/24: interface name;
30: change in port priority (default: 10)
------------------------------------------------------------------------------
>vrrp 1 priority 120

Configure the priority of VRRP backup group to 120. The greater the value is,
the higher the priority will be.
1: backup group number (1-255);      120: priority value (default: 100)
------------------------------------------------------------------------------
>vrrp 1 timers advertise 3

Configure the interval of advertising the VRRP on the IPv4 master routing device
 to 3s
1: backup group number (1-255) ;        3: interval of advertising the VRRP(def-
ault: 1)
------------------------------------------------------------------------------
>vrrp 1 track 192.168.217.1 interval 10

Configure the IP address monitored by the IPv4 VRRP backup group;
192.168.217.1: the IP address to be monitored;
10: the interval of detecting whether this destination address is reachable(def-
ault: 3)
------------------------------------------------------------------------------
```

Note

You can switch the interface language between Chinese and English by running **language {Chinese|English}** in privileged EXEC mode.

Related Commands

Command	Description
-	-

Platform Description

This command is supported on layer-3 switches but not on routers.

Command History

Version	Description
10.4(3)	New command

vrrp help

Use this command to show command instances that start with **vrrp** in interface configuration mode.

vrrp help

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples

- Chinese interface

```
Ruijie(config-VLAN 1)#vrrp help

命令举例：
------------------------------------------------------------------------------
>vrrp 1 ip 192.168.217.100

启用VRRP备份组1，设置该组的Primary IP地址为192.168.217.100；
1：  备份组号（1-255）；        192.168.217.100：IP地址；
------------------------------------------------------------------------------
>vrrp 1 priority 120

设置VRRP备份组的优先级为120，数值越大则优先级越高；
1：  备份组号（1-255）；        120：优先级（默认值：100）
------------------------------------------------------------------------------
```

- English interface

```
Ruijie(config-VLAN 1)#vrrp help

Examples:
------------------------------------------------------------------------------
>vrrp 1 ip 192.168.217.100

Enable the VRRP backup group 1 and set the primary IP address for this group 192
.168.217.100;
1:  backup group number (1-255);        192.168.217.100: IP address;
------------------------------------------------------------------------------
>vrrp 1 priority 120

Set the priority value for the VRRP backup group 120; the larger the priority
value is, the higher the priority is.
1:  backup group number (1-255);        120: priority value (default: 100)
------------------------------------------------------------------------------
```

Note

You can switch the interface language between Chinese and English by running **language {Chinese|English}** in privileged EXEC mode.

Related Commands

Command	Description
-	-

Platform This command is supported on layer-3 switches but not on routers.

Description

Command History	Version	Description
	10.4(3)	New command

view vrrp

Use this command to view the main VRRP status information.

view vrrp

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 command output:

```
Ruijie#view vrrp

Interface  Grp  Pri   timer  Own  Pre   State   Master addr       Group addr
---------  ---  ----  -----  ---  ----  ------  ---------------  -------------
VLAN 1     1    100   3      -    P     Init    0.0.0.0          1.1.1.1
Gi 0/1     1    100   -      -    P     Backup  192.168.201.213  192.168.201.1
Gi 0/1     2    120   -      -    P     Master  192.168.201.217  192.168.201.2
......
More information,refer to: show vrrp brief

Vrrp packet statistics
Total
  InReceives: 1000, InOctets: 1000000, InErrors: 50
  OutTransmits: 900, OutOctets: 900000
More infomation,refer to: show vrrp packet statistics
```

Related Commands	Command	Description
	vrrp help	Shows the typical VRRP configuration information.

Platform Description This command is supported on layer-3 switches but not on routers.

Command History

Version	Description
10.4(3)	New command

Hot-Plugging/ Unplugging Commands

Configuration Related Commands

The hot-plugging/unplugging involves the following commands:

install

remove

reset

show version slots

install

Use this command to install the line-card module.
Use the **no** form of this command to uninstall the line-card module.
install *slot-num moduletype*
no install *slot-num*

Parameter Description

Parameter	Description
slot-num	Slot number
moduletype	Module type

Command Mode Global configuration mode

Usage Guide This command is used to install the module driver manually. After the installation, all configurations for the slot will be done for the type of the installed module. Even if the module is unplugged, you can still configure it without loss of the configuration.
You can use this command to virtualize a specified type of line-card module and then configure this module. After the module is inserted, the configuration will take effect.
Use the **no** form of this command to uninstall the line-card module.

Configuration Examples The following example installs the module NMX-2GE line-card module in slot 2:

```
Ruijie(config)# install 2 NMX-2GE
```

Related Commands

Command	Description
N/A	N/A

Platform The **no install** command cannot be executed in SLAVE. There are not limits for the **install**

Description command.

Command History	Version	Description
	N/A	N/A

remove

Use this command to remove the line-card module configurations.
Use the **no** form of this command to restore the line-card module configurations.
remove *slot-num*
no remove *slot-num*

Parameter Description	Parameter	Description
	slot-num	Slot number

Command Mode Global configuration mode

Usage Guide This command must be executed before the line-card module is unplugged. Unplugging the line-card directly without executing the remove command will be considered as the abnormal unplugging, which has no damage to the hardware, but could lead to system failure with certain software status. The no remove command is used to restore the line-card module configurations after the remove command is executed without unplugging the line-card.

Configuration Examples The following example unplugs the line-card module in slot 2:

```
Ruijie(config)# remove 2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description The **no install** command cannot be executed in SLAVE.

Command History	Version	Description
	N/A	N/A

reset

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

Parameter Description

Parameter	Description
slot-num	Slot number

Command Mode Global configuration mode.

Usage Guide The hot plugging/unplugging resetting is equivalent to the combination of the following actions: remove, unplug the line-card, no install, install and plug the line-card.
After the reset configuration, the line-card executes the hardware resetting, and the software configurations are re-initialized.

Configuration Examples The following example resets the line-card module in slot 2:

```
Ruijie(config)# reset 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **no install** command cannot be executed in SLAVE.

Command History

Version	Description
N/A	N/A

Showing Related Command

show version slots

Use this command to show the details of the line-card modules, including the type of the line cards configured by users, the type of the inserted line cards, the hos swap status of the line cards, and information about MASTER and SLAVE.

3 status of the management board:

none- No management board is inserted in the slot;

slave- The management board in the slot is SLAVE.

MASTER- The management board in the slot is MASTER.

8 status of line cards:

- None: Neither a line card nor a pre-configured line card is in the slot.
- Installed: No line card is in the slot, but a line card is configured.
- running-config: MASTER is downloading configuration for the line card.
- running: The line card is running properly.
- run-remove: The user has run the **remove** command but has not removed the line card.
- conflict: The inserted line card is not the type pre-configured by the user.
- unins-remove: The user has run the **no install** command but has not removed the line card.
- standby: this status only works for the LPU expansion box and the device is SLAVE.

show version slots

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

Command Mode Privileged EXECmode.

Usage Guide This command is used to show the details of current line-card modules, such as the line-card type installed by users, actually installed line-card type, port number and current status.

Configuration Examples

Example 1: The following example shows the details of the “Two Hosts” modules:

```
Ruijie# show version slots
Dev  Slot   MaxPorts  Configured-Module  Online-Module    Status
    Peer-Status
---  ----   --------  ------------------ ---------------- ------
-----------
1    0/0    8         RSR30-X-SPU10      RSR30-X-SPU10    running
1    0/1    0                                             none
1    0/2    0         HNM-SEC            HNM-SEC          running
1    1/0    0         LPU-4HNM           LPU-4HNM         running        standby
1    1/1    0                                             none
1    1/2    0                                             none
1    1/3    0                                             none
1    1/4    0                                             none
1    2/0    0         LPU-4HNM           LPU-4HNM         standby    running
1    2/1    0                                             none
1    2/2    0                                             none
1    2/3    0                                             none
1    2/4    0                                             none
```

Example 2: The following example shows link faults in the mode of the “Two Hosts” mode:

```
Ruijie# show version slots
Dev  Slot   MaxPorts  Configured-Module  Online-Module    Status
    Peer-Status
---  ----   --------  ------------------ ---------------- ------
-----------
1    0/0    8         RSR30-X-SPU10      RSR30-X-SPU10    running
1    0/1    0                                             none
1    0/2    0         HNM-SEC            HNM-SEC          running
1    1/0    0         LPU-4HNM           LPU-4HNM         running
    running(error)
1    1/1    0                                             none
1    1/2    0                                             none
1    1/3    0                                             none
1    1/4    0                                             none
1    2/0    0         LPU-4HNM           LPU-4HNM         standby
standby(error)
1    2/1    0                                             none
1    2/2    0                                             none
1    2/3    0                                             none
1    2/4    0                                             none
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

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

Switchover

Use this command to manually switch MASTER and SLAVE.

switchover *slot-num*

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

Command Mode	Global configuration mode.
Usage Guide	"Two Hosts" mode is supported in RSR30-X series routers. LPU expansion boxes supported by RSR30-X series routers, such as LPU-4HNM expansion boxes, can be managed by two RSR30-X hosts with one host as MASTER and another as SLAVE. And the LPU expansion box is under the mangement of MASTER. MASTER/SLAVE switchover allows the previous SLAVE to perform management. Such switchover can be operated when this command is run in either host, after which, automatically, the former SLAVE switches to be MASTER and the former MASTER switches to be SLAVE. Note: In the **show version slot** command, the status of MASTER is displayed as "running" and that of SLAVE is "standby".
Configuration Examples	Example 1: The following example shows the MASTER/SLAVE switchover in Slot 1/0: `Ruijie(config)# switchover 1/0`

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

Platform Description	It is only supported in RSR30-X series routers.

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

Multi-link Load Balance Commands

Configuration Related Commands

Multi-link load balance configuration includes the following commands:

- **mllb enable**
- **mllb policy**
- **mllb policy intelligent**
- **mllb threshold**

mllb enable

Use this command to enable/disable the multi-link load balance in the global configuration mode .

mllb enable

no mllb enable

Parameter description	See the table below
Default configuration	The multi-link egress load balance function takes effect only for the default route of all zeros in the ECMP condition. For other routes in the ECMP condition, this function becomes invalid.
Command mode	Global configuration mode
Usage guidelines	N/A
Examples	The example enables the multi-link load balance function: `Ruijie# mll enable`
Related commands	See the table below
Platform description	N/A.

Parameter	Description
no	Disable the multi-link load balance function.

Command	Description
-	-

mllb policy

Use this command to configure the multi-link load balance policy in the global configuration mode.

mllb policy { **bandwidth | latency | load | intelligent**}

no mllb policy

Parameter description

Parameter	Description
bandwidth	Link-width-based multi-link load balance policy
latency	Access-latency-based multi-link load balance policy
load	Link-load-based multi-link load balance policy
intelligent	Multi-link load balance policy combining the link-bandwidth, access latency and link load.
no	Restore the multi-link load balance policy to the default value.

Default configuration

By default, it is the link-bandwidth-based multi-link load balance policy.

Command mode

Global configuration mode

Usage guidelines

The multi-link load policy can only be one of the **bandwidth, latency, load, intelligent**. To switch the policy to the other one, use the **mllb policy** command setting a new multi-link load balance policy. Use the **no mllb policy** command to restore the multi-link load balance policy to **bandwidth**.

Latency policy collects the latency information of destination IP through the flow, this policy cannot work before the latency information of destination IP is detected. So, when this destination IP creates the new flow for the first time, the multi-link egress load balance does not take effect.

Examples

The example configures the multi-link load balance policy as **load**:

```
Ruijie(config)#  mllb policy load
```

The example restores the multi-link load balance policy to the default value:

```
Ruijie(config)# no mllb policy load
```

Related commands

Command	Description
mllb enable	Enable the multi-link load balance function.
bandwidth	Set the link bandwidth.

Platform description

N/A

mllb policy intelligent

Use this command to configure the weight base of the bandwidth, latency,and load.

mllb policy intelligent [bandwidth *base1* **] [latency** *base2* **] [load** *base3* **]**

no mllb policy intelligent

Parameter description

Parameter	Description
bandwidth	Link bandwidth weight base, in the range of 1 to 100.
latency	Access latency weight base, in the range of 1 to 100.
load	Link load weight base, in the range of 1 to 100
no	Restore the policy to the default value.

Default configuration

The default value of each weight base is 1.

Command mode

Global configuration mode

Usage guidelines

On condition that the **intelligent** is selected as the multi-link load balance policy, the total weight of the link is the sum of the bandwidth, latency and load weight. When calculating the total weight of the link, use the weight base to multiply the weight of the corresponding factor, and then add the products together. By adjusting the bandwidth, latency and load weight base can change the proportion of the effect the three factors on the total weight of the link. The default value of the each weight base is 1.

Examples

The example configures the multi-link load balance policy as **intelligent** and sets the bandwidth weight to 50, latency weight to 60,

load weight to 100:

```
Ruijie(config)# mllb policy bandwidth 50 latency 60 load 100
```

Related commands

Command	Description
mllb enable	Enable the multi-link load balance function.
bandwidth	Sete the link bandwidth.
mllb policy	Configure the multi-link load balance policy.

Platform description N/A.

mllb threshold

Use this command to configure the threshold of the multi-link load balance.

mllb threshold *percent*

no mllb threshold

Parameter description

Parameter	Description
percent	Percent value of the multi-link load threshold.
no	Restore the threshold to the default value.

Default configuration By default, the threshold is 100.

Command mode Global configuration mode

Usage guidelines The multi-link load threshold is the percent value in the integer range of 1 to 100

Examples 1.The example sets the multi-link load threshold to 95:

```
Ruijie(config)# mllb threshold 95
```

Related commands

Command	Description
mllb enable	Enable the multi-link load balance function.

Platform description	N/A

Showing Related Commands

show mllb config

Use this command to show the configuration about the multi-link load balance.

show mllb config

Parameter description	

Parameter	Description
-	-

Default configuration	N/A
Command mode	Privileged EXEC mode, and global configuration mode
Usage guidelines	This command is used to show the current configuration about multi-link load balance.

Examples	The example shows the current configuration about the multi-link load balance:
	`Ruijie(config)# show mllb config`
	`muti-link load balance configure:`
	`muti-link load balance state: enabled`
	`muti-link load balance threshold: 95`
	`muti-link load balance policy: intelligent`
	`bandwidth weight base = 100`
	`latency weight base = 100`
	`load weight base = 100`

Related commands	

Command	Description
mllb enable	Enable the multi-link load balance function.
mllb policy	Set the multi-link load balance policy.

Platform description	N/A

RNS &Track Commands

delay

Use this command to specify a period of time after which the tracked object status will change if the interface status changes.
Use the **no** form of this command to restore the default setting.
delay { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }
no delay

Parameter Description

Parameter	Description
up *seconds*	Sets the delay time from down to up in the range from 0 to 180. The unit is second.
down *seconds*	Sets the delay time from up to down in the range from 0 to 180. The unit is second.

Defaults There is no delay by default.

Command Mode Track configuration mode

Usage Guide The continual oscillation of the tracked object status may cause the client of this tracked object changing also. This command can be used to delay advertising the change of the tracked object status. For example, the status of a tracked object changes from up to down, if the delay down 180 is configured, the down status will be advertised after 180 seconds. If the tracked object status changes to the up again in this period, it won't be advertised. For the client of the tracked object, the status of the tracked object is always up.

Configuration Examples The following example sets the delay time to 30 seconds when the tracked object changes to up from down.

```
Ruijie(config)# track 5 rns 10
Ruijie(config-track)# delay up 30
Ruijie(config-track)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

dns

Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode.

dns *destination-hostname* **name-server** *a.b.c.d*

Parameter Description

Parameter	Description
destination-hostname	Sets the destination IP address or the destination host domain name.
a.b.c.d	Sets the IP address for the DNS server.

Defaults N/A

Command Mode IP RNS configuration mode

Usage Guide Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode. If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

Configuration Examples The following example sets the IP RMS object to send the DNS packets.

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# dns www.ruijie.com.cn name-server 61.154.22.41
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

frequency

Use this command to set the interval of sending the packets, which must be no smaller than the timeout time.

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

frequency *milliseconds*

no frequency

Parameter Description

Parameter	Description
milliseconds	Sets the interval of sending the packets, in the range from10 to 604,800,000 in the unit of milliseconds.

Defaults The default is 60 seconds.

Command Mode IP RNS ICMP echo configuration mode
IP RNS DNS configuration mode
IP RNS UDP echo configuration mode

Usage Guide Use this command to set the interval of sending the ICMP echo or DNS packets, which must accord with the following formula to ensure accuracy:
frequency *milliseconds* > **timeout** *milliseconds* >= **threshold** *milliseconds*

Configuration Examples The following example configures an ICMP echo probe whose destination address is 192.168.21.1. The frequency, timeout time and threshold are set to 30,000, 8,000 and 6,000 milliseconds respectively.

```
Ruijie(config-ip-rns)#icmp-echo 192.168.21.1
Ruijie(config-ip-rns-icmp-echo)#frequency 30000
Ruijie(config-ip-rns-icmp-echo)#timeout 8000
Ruijie(config-ip-rns-icmp-echo)#threshold 6000
```

Related Commands

Command	Description
timeout	Defines the timeout time of sending the packets.

Platform Description N/A

icmp-echo

Use this command to configure an ICMP echo RNS probe.
icmp-echo { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] }
[**source-ipaddr** *ip-address*] [**out-interface** *type num* [**next-hop** *A.B.C.D*]]

Parameter Description

Parameter	Description
destination-hostname	Sets the destination IP address for the ICMP echo packets.
destination-hostname	Sets the destination host name within 127 characters. The exceeding characters are truncated automatically.
name-server *ip-address*	Sets the domain name server. The default domain name server is configured via the **ip name-server** command.
source-ipaddr *ip-address*	Sets the source IP address for the ICMP echo packets.
out-interface *type num*	Sets the outgoing port for the probe packet.
next-hop *A.B.C.D*	Sets the next hop IP address.

Defaults N/A

Command Mode IP RNS configuration mode

Usage Guide This command is used to enable the IP RNS object to send ICMP echo packets containing the specified destination IP address. The default payload size of an ICMP echo packet is 36 bytes. The **request-data-size** command is used to modify the packet size.
You can modify the probe parameter after specifying the type of the IP RNS probe (such as ICMP echo probe). If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

Configuration Examples The following example enables the IP RNS object to send the ICMP echo packets containing the destination IP address 10.1.1.1.

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ip rns

Use this command to define an IP RNS operation object and to enter the IP RNS configuration mode. Use the **no** form of this command to delete an IP RNS operation object.
ip rns *operation-number*
no ip rns *operation-number*

Parameter Description

Parameter	Description
operation-number	Sets the IP RNS operation object number, in the range from 1 to 500.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to define an IP RNS operation object and to enter the IP RNS configuration mode. At present, IP RNS probe only supports IPv4 upon 500 objects at most, which depends on device performance. As a value-added feature, too much IP RNS probe may lead in system overload. As a result, it will be disabled for the time being, ensuring normal function of core services (e.g. routing). After the IP RNS configuration mode is enabled, the probe object will not be created unless the probe

type is configured. If the type is set and object is created, use the **ip rns schedule** command to configure the startup policy, or the probe cannot be performed; use the **ip rns** command to enter the sub mode. If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

Configuration Examples The following example defines the IP RNS object 1.

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

Related Commands

Command	Description
show ip rns statistics	Displays the statistical data on the IP RNS object.

Platform Description N/A

show ip rns configuration

Use this command to display the RNS instance configuration.

show ip rns configuration [*operation-number*]

Parameter Description

Parameter	Description
operation-number	Sets the RNS instance number, in the range from 1 to 500.

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the RNS instance configuration. The configuration varies with different packet types.

Configuration Examples The following example displays the RNS 1 configuration.

```
Ruijie# show ip rns configuration 1
Entry number: 1
Tag: ruijie555
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 10000
Threshold (milliseconds): 5000
Recurring (Starting Everyday): FALSE
Life (seconds): 3500
Next Scheduled Start Time:Start Time already passed
```

```
Target address/Source address: 2.2.2.3/0.0.0.0
Request size (ARR data portion): 36
```

Field	Description
Entry number	IP RNS operation index
Tag	Instance tag.
Type of operation to perform	Operation type.
Operation timeout (milliseconds)	Operation timeout.
Operation frequency (milliseconds)	Operation frequency.
Threshold (milliseconds)	Threshold.
Recurring (Starting Everyday)	The operation starts every day.
Life (seconds)	Life time
Next Scheduled Start Time	Next scheduled start time.
Target address/Source address	Target address/Source address
Request size (ARR data portion)	Request packet size.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip rns statistics

Use this command to display the RNS object statistics.

show ip rns statistics [*operation-number*]

Parameter Description

Parameter	Description
operation-number	Sets the IP RNS operation object number, in the range from 1 to 500

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The statistics vary with different packet types.

Configuration Examples The following example displays the RNS object statistics.

```
Ruijie#show ip rns statistics 1
Round trip time(RTT) Index 1
Operation time to live: Forever
Latest RTT: 1 ms
Latest operation start time: 2014-01-20 10:21:38
```

```
Latest operation return code: OK
Number of successes: 386
Number of failures: 12
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

show track

Use this command to display statistics of the tracked object.

show track [*track-number*]

Parameter Description	Parameter	Description
	track-number	Sets the tracked object number, in the range from 1 to 700.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays statistics of all tracked objects.

```
Ruijie#show track
Track 1
  Reliable Network Service 5
  The state is Up
    1 change, current state last: 120 secs
  Delay up 30 secs, down 50 secs
Track 3
  Interface FastEthernet 1/0
  The state is Down, delayed Up (5 secs remaining)
    3 change, current state last: 300 secs
  Delay up 60 secs, down 60 secs
Track 4
  List boolean and
  Object 1
  Object 2 not
  The state is Up
```

```
 1 change, current state last: 100 secs
 Delay up 0 secs, down 0 secs
```

Field	Description
Track x	Tracked object ID
Reliable Network Service x	Tracked RNS object
The state is x	Tracked object state
x change	Tracked object change count
current state last: x secs	The time for which the current state lasts
Delay up x secs, down x secs	The delay state of the tracked object
Interface x x	Tracked interface
The state is x, delayed y (c secs remaining)	The tracked object state is x, and will turn to y in c seconds.
List boolean and	The Boolean expression enables calculation by using “and” operator.
Object x	Object x is in the up state.
Object x not	Object x is in the down state.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

timeout

Use this command to set the timeout time of an IP RNS probe.
Use the **no** form of this command to restore the default setting.
timeout *milliseconds*
no timeout

Parameter Description

Parameter	Description
milliseconds	Sets the timeout time, in the range from 10 to 604,800,000 in the unit of milliseconds. The default is 5,000 milliseconds.

Defaults The default timeout of an IP RNS probe varies with the detection type, which can be displayed by using **show ip rns configuration** command.

Command Mode
IP RNS ICMP echo configuration mode
IP RNS DNS configuration mode
IP RNS configuration mode

Usage Guide The timeout value must be no smaller than the threshold value. See **Usage Guide** of the **frequency** command for the relationship among timeout, frequency and threshold.

Configuration Examples The following example sets the timeout time of an IP RNS probe to 10,000 milliseconds.

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# timeout 10000
Ruijie(config-ip-rns-icmp-echo)# exit
```

Related Commands

Command	Description
frequency *milliseconds*	Sets the interval of sending the packets.

Platform Description N/A

IPv6 Configuration Commands

IPv6 Commands

ping ipv6

Use this command to diagnose the connectivity of an IPv6 network.

ping ipv6 [*ipv6-address*]

Parameter Description

Parameter	Description
ipv6-address	Destination IP address to be diagnosed

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If no destination address is entered in the command, user interaction mode is entered, and you can specify the parameters. The following table shows the meanings of symbols returned by the **ping** command:

Signs	Meaning
!	The response to each request sent is received.
.	The response to the request sent is not received within a specified time.
U	The device has no route to the destination host.
R	Parameter error.
F	No system resource is available.
A	The source IP address of the packet is not selected.
D	The network interface is in the DOWN state, or the IPv6 function is disabled on the network interface (for example, a duplicate IP address is detected).
?	Unknown error.

Configuration Examples

```
Ruijie# ping ipv6 fec0::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description

N/A	N/A

ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to delete the configured address.

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
ipv6-address	IPv6 address in the format defined in RFC 4291. The address must be in hex; the fields in the address must be separated by a comma, and each field must contain 16 bits.
ipv6-prefix	IPv6 address prefix in the format defined in RFC 4291. The address must be in hex; the fields in the address must be separated by a comma, and each field must contain 16 bits.
prefix-length	Length of the IPv6 prefix, the network address of the IPv6 address.
prefix-name	The general prefix name. Use the specified general prefix to generate the interface address.
sub-bits	The value of the sub-prefix bits and the host bits. The value combines with the general prefix to generate the interface address. The value must be in the format defined in RFC 4291.
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

If the interface is bound to a multi-protocol VRF that is not configured with an IPv6 address family, it is not allowed to configure an IPv6 address for the interface. In this case, you must configure an IPv6 address family for the multi-protocol VRF before configuring an IPv6 address for the interface.

Usage Guide When an IPv6 interface is created and the link state is UP, the system will automatically generate a link-local IP address for the interface.

The IPv6 address can also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bits. The general prefix can be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 client prefix discovery (PD) function (see the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this

command to configure the sub-prefix and the host bits.

If no deleted address is specified you use **no ipv6 address**, all the manually configured addresses will be deleted.

no ipv6 address *ipv6-prefix*/*prefix-length* **eui-64** can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix*/*prefix-length* **eui-64**.

Configuration Examples

The following example configures IPv6 addresses manually.

```
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
```

The following example uses a general prefix to configure an address.

```
Ruijie(config-if)# no ipv6 address 2002:1::1/64 eui-64
```

Assuming that the general prefix my-prefix is configured as 2001:1111:2222::/48, the IPv6 address generated for the interface is 2001:1111:2222:7272::72/64.

Related Commands

Command	Description
ipv6 address autoconfig	Automatically configures a stateless address.
ipv6 general-prefix	Configures the general prefix.
show ipv6 general-prefix	Displays the general prefix.

Platform Description

This command is supported on all platforms.

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 delete the automatically configured address.

ipv6 address autoconfig [default]

no ipv6 address autoconfig

Parameter Description

Parameter	Description
default	(Optional) If this keyword is configured, a default route is generated. Note that only one layer-3 interface on the entire device is allowed to use the **default** keyword

Defaults

N/A

Command Mode

Interface configuration mode

If the interface is bound to a multi-protocol VRF that is not configured with an IPv6 address family, it is not allowed to enable the IPv6 stateless address auto configuration function on the interface. In this case, you must configure an IPv6 address family for the multi-protocol VRF before enabling the IPv6 stateless address auto configuration function.

Usage Guide

The stateless address auto configuration is that when receiving a route advertisement (RA) message,

the device can use the prefix information of the RA message to automatically generate the EUI-64 interface address.

If the RA message contains the other-config-flag, the interface will obtain these other configurations through DHCPv6. The other configurations usually mean 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 of the interface.

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 an IPv6 address for the interface manually.

Platform Description The command is supported on all platforms.

ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to disable this function.

ipv6 enable

no ipv6 enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The IPv6 function of the interface 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 an IPv6 address for the interface.

If the interface is bound to a multi-protocol VRF that is not configured with an IPv6 address family, it is not allowed to enable the IPv6 function on the interface. In this case, you must configure an IPv6 address family for the multi-protocol VRF before enabling the IPv6 function.

Caution 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

```
Ruijie(config-if)# ipv6 enable
```

Examples

Related Commands	**Command**	**Description**
	show ipv6 interface	Displays the related information of an interface.

Platform Description N/A

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

ipv6 general-prefix

Use this command to configure an IPv6 general prefix in 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	General prefix name
	pv6-prefix	Network prefix value of the general-prefix following the format defined in RFC 4291
	prefix-length	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 can refer to it. These specified prefixes are updated whenever the general prefix changes. If the network ID changes, just modify the general prefix.
A general prefix can contain multiple prefixes.
These longer specified prefixes are usually used for the IPv6 address configuration on the interface.

Configuration Examples The following example manually configures 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 This command is supported on all platforms.

Command History	Version	Description
	N/A	N/A

ipv6 hop-limit

Use this command to configure the default hop count to send unicast messages in global configuration mode.

ipv6 hop-limit *value*

no ipv6 hop-limit

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The default value is 64.

Command Mode Global configuration mode

Usage Guide This command is effective for unicast messages only, and not effective for multicast messages.

Configuration Examples

```
Ruijie(config)# ipv6 hop-limit 100
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

Command History	Version	Description
	N/A	N/A

ipv6 mtu

Use this command to set the maximum transmission unit (MTU) of IPv6 packets on the interface. Use the **no** form of this command to restore the default settings.

ipv6 mtu *bytes*

no ipv6 mtu

Parameter Description	Parameter	Description
	bytes	IPv6 MTU within the range from 1280 to 1500 bytes.

Defaults The default value is the same as the default IPv4 MTU.

Command Mode Interface configuration mode

Usage Guide If an IPv6 packet exceeds its MTU, RGOS software will split the packet, All devices in the same physical segment share the same IPv6 MTU.

Configuration Examples The following example sets IPv6 MTU on 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 IPv4 MTU on the interface

Platform Description This command is not supported on layer-2 devices.

ipv6 nd dad attempts

Use this command to set the number of the neighbor solicitation (NS) messages to be continuously sent for duplicate IPv6 address detection on the interface. Use the **no** form of this command to restore the default setting.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts

Parameter Description

Parameter	Description
value	Number of the NS messages. If it is set to 0, it indicates that duplicate IPv6 address detection is disabled on the interface. The range is 0 to 600.

Defaults 1

Command Mode Interface configuration mode

Usage Guide When the interface is configured with a new IPv6 address, duplicate address detection (DAD) must be enabled before the address is assigned to the interface, and the address is in the TENTATIVE state. After the DAD is completed, if no duplicate IP address is detected, the address can be used normally; if a duplicate IP address 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 must modify and configure a new address manually, and change the interface status from DOWN to UP to restart DAD for the interface. Whenever the status of an interface changes from DOWN to UP, the DAD function of the interface will be enabled.

Configuration

```
Ruijie(config-if)# ipv6 nd dad attempts 3
```

Examples

Related Commands	**Command**	**Description**
	show ipv6 interface	Displays the interface information.

Platform Description N/A

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

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 remove the setting.

ipv6 nd managed-config-flag

no ipv6 nd managed-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 This flag bit determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag bit is set, the host obtains an IP address through stateful auto configuration; otherwise the IP address is not obtained through stateful auto configuration.

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 bit for obtaining all information except IP address through stateful auto configuration.

Platform Description N/A

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

ipv6 nd other-config-flag

Use this command to set the **other stateful configuration** flag bit of the RA message. Use the **no** form of this command to remote the setting.

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 DHCPv6 to obtain the information excluding the IPv6 address for the purpose of performing auto configuration. When the **managed address configuration** is set, the **other stateful configuration** is also set by default.

Configuration Examples

```
Ruijie(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Displays the RA information of the interface.
ipv6 nd managed-config-flag	Sets the **managed address configuration** flag bit of the RA message.

Platform Description N/A

Command History

Version	Description
N/A	N/A

ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmit an NS. 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 an NS in the range of 1000 to 429467295 milliseconds

Defaults The default value in the RA is 0 (unspecified); the interval for retransmitting an NS in neighbor discovery is 1000 milliseconds (1 second).

Command mode Interface configuration mode

Usage Guide The configured value will be advertised through a RA and will be used by the device itself. It is recommended that the value should not be set to 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

Command History	Version	Description
	N/A	N/A

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 it to 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 RFC 4291.
	prefix-length	Length of the IPv6 prefix. A slash (/) must be added before 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 of 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	Indicates that 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 The advertised prefix is the one set with **ipv6 address** on the interface by default. The default parameters of the prefix configured in the RA are as follows:
valid-lifetime: 2592000 seconds (30 days)
preferred-lifetime: 604800 seconds (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. The prefix advertised in the RA is the one set with **ipv6 address** on the interface by default. 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, 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 way, the valid lifetime of the prefix sent in each 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 parameters of the prefix for SVI 1 (the parameters 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

Command History	Version	Description
	N/A	N/A

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	Lifetime of the default device on the interface

Defaults 1800 seconds

Command Mode Interface configuration mode

Usage Guide The device lifetime field is available in each RA. It specifies the time during which the hosts on 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 the value is not set to 0, it must be larger than or equal to the interval for sending the RA (ra-interval).

Configuration Examples

```
Ruijie(conifig-if)# ipv6 nd ra-lifetime 2000
```

Related Commands	Command	Description
	show ipv6 interface	Displays the RA information of the interface.
	ipv6 nd ra-interval	Sets the interval for sending the RA.
	ipv6 nd ra-hoplimit	Sets the hop count of the RA.
	ipv6 nd ra-mtu	Sets the MTU of the RA.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

ipv6 nd ra-interval

Use this command to set the interval for sending the RA on the interface. 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 for sending the RA message in seconds
min-max	Maximum and minimum intervals for sending the RA message
min_value	Minimum interval for sending the RA message
max_value	Maximum interval for sending the RA message

Defaults The default value is 200 seconds. The actual interval for sending the RA message is 200 multiplied by 1.2 or 0.8.

Command Mode Interface configuration mode

Usage Guide If the device serves as the default device, the set interval cannot be longer than the lifetime of the device. Besides, to ensure other devices on the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message is the set value multiplied by 1.2 or 0.8. If the keyword **min-max** is specified, the actual interval for sending the packet will be chosen between the 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 RA information of the interface.
ipv6 nd ra-lifetime	Sets the lifetime of the device.
ipv6 nd ra-hoplimit	Sets the hop count of the RA message.
ipv6 nd ra-mtu	Sets the MTU of the RA message.

Platform Description N/A

Command History

Version	Description
N/A	N/A

ipv6 nd ra-hoplimit

Use this command to set the hop count of the RA message sent on the interface. 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	Hop count of the RA message

Defaults The default value is 64.

Command Mode Interface configuration mode

Usage Guide Use this command to set the hop count of the RA message.

Configuration Examples

```
Ruijie(config -if)# ipv6 nd ra-hoplimit 110
```

Related Commands	Command	Description
	show ipv6 interface	Displays the RA information of the interface.
	ipv6 nd ra-lifetime	Sets the lifetime of the device.
	ipv6 nd ra-interval	Sets the interval for sending the RA message.
	ipv6 nd ra-mtu	Sets the MTU of the RA message.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

ipv6 nd ra-mtu

Use this command to set the MTU of the RA message sent on the interface. 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 RA message

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 RA information of the interface.
ipv6 nd ra-lifetime	Sets the lifetime of the device.
ipv6 nd ra-interval	Sets the interval for sending the RA message.
ipv6 nd ra-hoplimit	Sets the hop count of the RA message.

Platform Description N/A

Command History

Version	Description
N/A	N/A

ipv6 nd reachable-time

Use this command to set the time during which the neighbor is considered as reachable 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	The reachable time of the neighbor, in the range of 0 to 3600000 milliseconds.

Defaults The default value in the RA is 0 (unspecified); the reachable time of the neighbor in neighbor discovery is 30000 milliseconds (30 seconds).

Command Mode Interface configuration mode

Usage Guide The device detects unavailable neighbors by using the set time. If the set time is shorter, the device can detect the failure of a neighbor faster, but more network bandwidth is wasted, and more resources of the device are consumed. Therefore, it is recommended that the value should not be set to a too short time.

The configured value will be advertised through a RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.

Configuration Examples Ruijie(config-if)# ipv6 nd reachable-time 1000000

Related

Command	Description

Commands	show ipv6 interface	Displays the interface information.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message. Use the **no** form of this command to enable the interface to send the RA message.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The RA message is not sent on the IPv6 interface 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 Commands	Command	Description
	show ipv6 interface	Displays the RA information of the interface.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to remove the setting.

ipv6 neighbor *ipv6-address interface-id hardware-address*

no ipv6 neighbor *ipv6-address interface-id*

Parameter Description

Parameter	Description
ipv6-address	IPv6 address of the neighbor. It must follow the address format defined in RFC 4291.
interface-id	Network interface of the neighbor (including routed Port, L3 AP interface, or SVI interface).
hardware-address	Hardware address of the neighbor. It must be a 48-bit MAC address in the format of XXXX.XXXX.XXXX, where “X” is a hexadecimal number.

Defaults No static neighbor is configured.

Command Mode Global configuration mode

Usage Guide Similar to the ARP command, this command can only be used to configure a static neighbor on an IPv6 protocol enabled interface.

If the neighbor to be configured has been learned through NDP and has been stored in the neighbor table, the dynamically generated neighbor will be automatically switched to a static one. The configured static neighbor is always in the REACHABLE state if it is valid. An invalid static neighbor is a static neighbor configured with an IPv6 address not matching the address configured on the interface (the IPv6 address is not in any IPv6 address section of the interface or conflicts with the interface address), and in this case, packets will not be forwarded according to the MAC address specified by the static neighbor. The invalid static neighbor is in the INACTIVE state. You can use **show ipv6 neighbor static** to view the availability status of the static neighbor.

Use **clear ipv6 neighbors** to clear all the neighbors dynamically learned through NDP.

Use **show ipv6 neighbors** to view the neighbor information.

Configuration Examples

```
Ruijie(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related Commands

Command	Description
show ipv6 neighbors	Displays the neighbor information.
clear ipv6 neighbors	Clears the neighbors learned dynamically.

Platform Description N/A

Command History

Version	Description
N/A	N/A

ipv6 ns-linklocal-src

Use this command to set the link-local address as the source IP address to send an NS. When **no ipv6 ns-linklocal-src** is executed, the link-local address or the global unicast address will be selectively used according to the destination IPv6 address as the source IP address to send an NS, as specified in RFC 3484.

ipv6 ns-linklocal-src

no ipv6 ns-linklocal-src

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

Defaults The link-local address is always used as the source address to send an NS.

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

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

ipv6 redirects

Use this command to control whether to send an ICMPv6 redirect message when the device receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to disable the function.

ipv6 redirects

no ipv6 redirects

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

Defaults The ICMPv6 redirect message is permitted to be sent on the IPv6 interface.

Command Mode Interface configuration mode

Usage Guide The transmission rate of each ICMPv6 error message is limited. It is 10 pps by default.

Configuration Examples

```
Ruijie(config-if)# ipv6 redirects
```

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.

Platform Description N/A

Command History	Version	Description
	N/A	N/A

ipv6 route

Use this command to configure an IPv6 static route. Use the **no** form of this command to remove the setting.

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface-id* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance*] [**weight** *number*]

Parameter Description

Parameter	Description
vrf-name	VRF in the route, which must be the multi-protocol VRF with the IPv6 address family configured.
ipv6-prefix	IPv6 prefix following the format specified in RFC 4291.
prefix-length	Length of the IPv6 prefix. A slash (/) must be added before the prefix.
ipv6-address	Next-hop IP address to the destination network. It must be in the format defined in RFC 4291. The next-hop IP address and the next-hop outgoing interface can be specified at the same time. Note that if the next-hop IP address is a link-local address, the outgoing interface must be specified.
interface-id	The outgoing interface to the destination network. If the static route is configured with the outgoing interface but no next-hop address is specified, the destination address will be considered to be on the link connected with the outgoing interface; that is, the static route will be treated as a direct route. Note that if the destination network or next-hop address is a link-local address, the outgoing interface must be specified.
vrf-name1	VRF in the next hop, which must be the multi-protocol VRF with the IPv6 address family configured.
default	The next hop is global.
distance	(Optional) Administrative distance for the static route.
number	(Optional) Weight of the static route. When an equal-cost path is configured, the parameter specifies the weight of the path. The range is 1 to 32. The sum of weights of all equal-cost paths for a route cannot be greater than the maximum number of equal-cost paths that can be configured for the route. The ratio of weights of equal-cost paths for a route specifies the ratio of traffic of the paths.

Defaults N/A

Command Mode Global configuration mode

When the IPv6 address family of a multi-protocol VRF is deleted, IPv6 static routes in the VRF and IPv6 static routes whose next-hop VRF is the VRF are deleted.
Assuming that an IPv6 static route is configured with an interface and a next-hopVRF, if the VRF bound to the interface is inconsistent with the next-hop VRF, the configuration does not take effect.

Usage Guide


Note

1. If the destination IP address or next-hop IP address is a link-local IP address, the outgoing interface must be specified; if the destination address is a link-local IP address, the next-hop must also be a link-local IP address. When a route is configured, the destination IP address and the next-hop IP address cannot be a multicast address. If both the next hop IP address and the outgoing interface are specified, the outgoing interface of the direct route that matches the next hop must be the same as the configured outgoing interface.

Configuration Examples The following example configures a global IPv6 route.

```
Ruijie(config)# ipv6 route 2001::/64 vlan 1 2005::1
```

The following example configures an inter-VRF IPv6 route from vrf1 to vrf2, where the route prefix belongs to vrf1, but the next hop belongs to vrf2.

```
Ruijie(config)# vrf definition vrf1
Ruijie(config-vrf)# address-family ipv6
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config)# vrf definition vrf2
Ruijie(config-vrf)# address-family ipv6
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config-vrf)# ipv6 route vrf vrf1 2001::/64 1000::1 nexthop-vrf vrf2
```

The following example configures an IPv6 route from a VRF to a global address, where the route prefix belongs to vrf1, the exit is an IPv6 over IPv4 manual tunnel, and the tunnel interface is global.

```
Ruijie(config)# vrf definition vrf1
Ruijie(config-vrf)# address-family ipv6
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config-vrf)# interface tunnel 1
Ruijie(config-if)# ipv6 address 1000::1/64
Ruijie(config-if)# tunnel mode ipv6ip
Ruijie(config-if)# tunnel source 1.1.1.1
Ruijie(config-if)# tunnel destination 1.1.1.2
```

```
Ruijie(config-if)# ipv6 route vrf vrf1 2000::/64 tunnel 1
```

Related Commands	Command	Description
	vrf definition	Defines a multi-protocol VRF.
	show ipv6 route	Displays the IPv6 route information.

Platform Description N/A

Command History	Version	Description
	10.1	The command is introduced for the first time.
	10.4	The *weight* parameter is added.
	10.4(3)	The parameters **vrf** *vrf-name* and **nexthop-vrf** {*vrf-name1*| **default**} are supported and tested.

ipv6 source-route

Use this command to forward the IPv6 packet with a route header. Use the **no** form of this command to disable the forwarding function.

ipv6 source-route

no ipv6 source-route

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The function is disabled by default.

Command Mode Global configuration mode

Usage Guide Because of the security issues of type 0 route headers, the device is vulnerable to the denial of service attack. Therefore, forwarding the IPv6 packet with a route header is disabled by default. However, the IPv6 packet with a type 0 route header destined for 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

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

tunnel destination

Use this command to specify the destination address for the tunnel. Use the **no** form of this command to remove the setting.

tunnel destination { *ipv4-address* | *ipv6-address* }

no tunnel destination

Parameter Description	**Parameter**	**Description**
	ipv4-address	Destination address of the tunnel, namely, the IPv4 address at the other end of the tunnel.
	ipv6-address	Destination address of the tunnel. If the tunnel mode ipv6 is configured, the destination address of the tunnel must be an IPv6 address. If the tunnel mode gre ipv6 is configured, the destination address of the tunnel must also be an IPv6 address.

Defaults	The destination address encapsulated by the tunnel is not configured by default.
Command Mode	Interface configuration mode
Usage Guide	A device cannot be configured with multiple tunnels with the same encapsulation type, source address and destination address. Note: For auto tunnels (6to4 and ISATAP), the destination address cannot be configured.
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 source	Configures the source IP address of the tunnel.
	tunnel mode	Configures the mode of the tunnel.
	Tunnel ttl	Configures the TTL of the tunnel.

Platform Description	N/A

Command	**Version**	**Description**

History	10.4(1)	The *ipv6-address* parameter is supported and tested.

tunnel mode ipv6

Use this command to configure a static IPv6 tunnel, which can carry an IPv4 or IPv6 message. Use the **no** form of this command to restore default tunnel mode.

tunnel mode ipv6

no tunnel mode

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The default mode is ipv6ip.

Command mode Interface configuration mode

Usage Guide Use this command to configure the 4over6 or 6over6 static tunnel.

Configuration Examples The following is a configuration example.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel mode ipv6
Ruijie(config-if)# tunnel source vlan 1
```

Related Commands	Command	Description
	tunnel source	Configures the source address of the tunnel.
	tunnel destination	Configures the destination address of the tunnel.
	Tunnel ttl	Configures the TTL of the tunnel.

Platform Description The command is supported by switches, but not by routers.

Command History	Version	Description
	10.4(1)	The command is supported and tested.

tunnel mode ipv6ip

Use this command to configure static IPv6 tunnel mode. Use the **no** form of this command to restore default IPv6 tunnel mode.

tunnel mode ipv6ip [**6to4** | i**satap**]

no tunnel mode

Parameter Description	Parameter	Description
	6to4	Configures the tunnel as an auto 6to4 tunnel.

isatap	Configures the tunnel as an auto ISATAP tunnel.

Defaults The type of the configured IPv6 tunnel is a tunnel configured manually.

Command Mode Interface configuration mode

Usage Guide After a tunnel is created, it is considered to be a manual tunnel by default. You can also use **tunnel mode ipv6ip** without any parameter to set a tunnel to a manual tunnel. For an auto tunnel, no destination address is specified.

Configuration Examples The following example configures a 6to4 tunnel.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel mode ipv6ip 6to4
```

Related Commands

Command	Description
tunnel source	Configures the source address of the tunnel.
tunnel destination	Configures the destination address of the tunnel.
Tunnel ttl	Configures the TTL of the tunnel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

tunnel mode gre

Use this command to configure GRE tunnel mode. Use the **no** form of this command to restore default IPv6 tunnel mode.

tunnel mode gre [**ip** | **ipv6**]

no tunnel mode

Parameter Description

Parameter	Description
ip	Configures the protocol of the tunnel as IPv4.
ipv6	Configures the protocol of the tunnel as IPv6.

Defaults The type of the configured IPv6 tunnel is a tunnel configured manually.

Command Mode Interface configuration mode

Usage Guide After a tunnel is created, it is considered to be a manual tunnel by default. You can also use **tunnel mode gre** with the **ip** or **ipv6** option to set a tunnel to a GRE tunnel. The GRE tunnel is able to be up only when the tunnel source and tunnel destination are configured and the destination route is

reachable.

Configuration Examples The following example configures a GRE tunnel.

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel mode gre ip
Ruijie(config-if)# tunnel source vlan 1
Ruijie(config-if)# tunnel destination 1.1.1.1
```

Related Commands

Command	Description
tunnel source	Configures the source address of the tunnel.
tunnel destination	Configures the destination address of the tunnel.
tunnel ttl	Configures the TTL of the tunnel.

Platform Description N/A

Command History

Version	Description
10.4(2)	The **ipv6** parameter is supported and tested.

tunnel source

Use this command to specify the source IP address for the tunnel. Use the **no** form of this command to remove the 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 must be an IPv6 address. Using the link-local address as the source address is not supported currently.
interface-type interface-number	Interface referenced by the source IP address of the tunnel. If the tunnel mode is ipv6ip, the primary IPv4 address of the referenced interface will be used as the source IPv4 address of the packets to be transmitted through the tunnel. If the tunnel mode is ipv6, the first IPv6 global unicast address of the referenced interface will be used as the source IPv6 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 that the source address should be specified.
A device cannot be configured with multiple tunnels with the same encapsulation type, source address and destination address.
If there are multiple auto tunnels, their source addresses must 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 the tunnel.
tunnel destination	Configures the destination address of the tunnel.
Tunnel ttl	Configures the TTL of the tunnel.

Platform Description N/A

Command History

Version	Description
10.4(1)	The *ipv6-address* parameter is supported and tested.

tunnel ttl

Use this command to specify the TTL value of an IPv4 packet in an IPv6 over IPv4 tunnel or set the hop limit of an IPv6 packet in an IPv4 over IPv6 tunnel or an IPv6 over IPv6 tunnel. Use the **no** form of this command to restore the default value of 255.
tunnel ttl *value*
no tunnel ttl

Parameter Description

Parameter	Description
value	TTL value

Defaults The default value is 128.

Command Mode Interface configuration mode

Usage Guide Use this command to specify the TTL value of an IPv4 packet in an IPv6 over IPv4 tunnel or set the hop limit of an IPv6 packet in an IPv4 over IPv6 tunnel or an IPv6 over IPv6 tunnel.

Configuration Examples

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if)# tunnel ttl 64
```

Related Commands

Command	Description
tunnel mode	Configures the mode of the tunnel.
tunnel source	Configures the source IP address of the tunnel.
tunnel destination	Configures the destination IP address of the tunnel.

Platform Description N/A

Command History

Version	Description
N/A	N/A

tunnel vrf

Use this command to configure the VRF to which the outer-layer addresses of a tunnel belong. The VRF routing table is used to forward packets to the tunnel interface.

tunnel vrf *vrf-name*

no tunnel vrf

Parameter Description

Parameter	Description
vrf-name	Name of the outer-layer VRF of the tunnel.

Defaults The outer-layer source and destination addresses of the tunnel are global addresses.

Command Mode Interface configuration mode

Usage Guide The outer-layer source and destination addresses of the tunnel must be in the same VRF. If the specified VRF does not include a route to the destination address, the tunnel interface is down.

If the outer-layer VRF of the tunnel is configured as an IPv4 VRF, for an IPv4/v6 over IPv6 tunnel or an IPv4/v6 over IPv6 GRE tunnel, the configuration of the outer-layer VRF of the tunnel is not effective, that is, the source and destination addresses of the tunnel are global addresses.

In the following description, it is assumed that the outer-layer VRF of the tunnel is configured as a multi-protocol VRF.

1) For a 6to4 tunnel or an ISATAP tunnel, if the multi-protocol VRF is not configured with an IPv4 address family, the link protocol status of the tunnel is DOWN.

2) For an IPv4/v6 over IPv4 tunnel or an IPv4/v6 over IPv4 GRE tunnel, if the multi-protocol VRF is not configured with an IPv4 address family, the VRF has no corresponding IPv4 routing table, the destination address of the tunnel is unreachable, and the link protocol status of the tunnel is DOWN.

3) For an IPv4/v6 over IPv6 tunnel or an IPv4/v6 over IPv6 GRE tunnel, if the multi-protocol VRF is not configured with an IPv6 address family, the VRF has no corresponding IPv6 routing table, the destination address of the tunnel is unreachable, and the link protocol status of the tunnel is DOWN.

Configuration Examples The following example specifies the outer-layer VRF of a manual IPv6 over IPv4 tunnel as IPv4 VRF red.

```
Ruijie(config)# ip vrf red
Ruijie(config-vrf)#exit
Ruijie(config)# interface tunnel 1
Ruijie(config-tunnel1)# tunnel mode ipv6ip
Ruijie(config-tunnel1)# tunnel vrf red
```

The following example specifies the outer-layer VRF of an IPv6 tunnel as multi-protocol VRF blue.

```
Ruijie(config)# ip vrf blue
Ruijie(config-vrf)# address-family ipv6
Ruijie(config-vrf-af)# exit-address-family
Ruijie(config-vrf)#exit
Ruijie(config)# interface tunnel 1
Ruijie(config-tunnel1)# tunnel mode ipv6
Ruijie(config-tunnel1)# tunnel vrf blue
```

Related Commands

Command	Description
ip vrf	Configures an IPv4 VRF.
tunnel mode	Configures the mode of the tunnel.
tunnel source	Configures the source IP address of the tunnel.
tunnel destination	Configures the destination IP address of the tunnel.
vrf definition	Configures a multi-protocol VRF.

Platform Description The command is supported on the routers only.

Command History

Version	Description
10.4(2)	The command is introduced.
10.4(3)	The command for configuring an outer-layer VRF for an IPv4/v6 over IPv6 tunnel and an IPv4/v6 over IPv6 GRE tunnel is supported and tested.

clear ipv6 neighbors

Use this command to clear the dynamically learned neighbors.

clrear ipv6 neighbors [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
vrf-name	VRF name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to clear all the neighbors dynamically learned by neighbor discovery. Note that the static neighbors will not be cleared.

Configuration Examples

```
Ruijie# clear ipv6 neighbors
```

Related Commands

Command	Description
ipv6 neighbor	Configures a neighbor.
show ipv6 neighbors	Displays the neighbor information.

Platform Description N/A

Command History

Version	Description
10.4(3)	The **vrf** *vrf-name* parameter is supported and tested.

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 addresses 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 interface of the device.

```
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

Command History	Version	Description
	10.4(3)	The command is added.

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 those manually configured and learned from the DHCPv6 client.

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 The command is supported by all platforms.

Command History

Version	Description
N/A	N/A

show ipv6 interface

Use this command to display the IPv6 interface information.

show ipv6 interface [*interface-id*] [**ra-info**]

Parameter Description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregate port, or SVI)
ra-info	Displays the RA information of the interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the address configuration, ND configuration and other statistical information of an IPv6 interface.

Configuration Examples

```
Ruijie# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
```

```
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds
```

- The following line is included in the above information:
- INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]

The flag bits in the square brackets [ ] following the INET6 address are described as follows:

Field	Description
ANYCAST	Indicates that the address is an anycast address.
TENTATIVE	Indicates that DAD is underway. The address is a tentative address before the DAD is completed.
DUPLICATED	Indicates that a duplicate address exists.
DEPRECATED	Indicates that the preferred lifetime of the address expires.
NODAD	Indicates that no DAD is implemented for the address.
AUTOIFID	Indicates that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.
PRE	Indicates a stateless address that is automatically configured.
GEN	Indicates an address generated by a general prefix.

```
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 router advertisements live for 1800 seconds
ND router 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)
```

The fields in **ra-info** are described as follows:

Field	Description
RA timer is stopped (on)	Indicates whether the RA timer is started.
waits	Indicates the number of RSs received but not acknowledged yet.
initcount	Indicates the number of RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: indicates the number of the RAs that are sent. In: indicates the number of the RAs that are received. inconsistent: indicates the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicates the number of the RSs that are received.
Link-layer address	Indicates the link-layer address of the interface.
Physical MTU	Indicates the link MTU of the interface.
!M | M	!M: indicates that the managed-config-flag bit in the RA is not set. M: indicates that the managed-config-flag bit in the RA is set.
!O | O	!O: indicates the other-config-flag bit in the RA is not set. O: indicates the other-config-flag bit in the RA is set.

The fields of the prefix list in **ra-info** are described as follows:

Field	Meaning
total	Indicates the number of the prefixes of the interface.
fec0:1:1:1::/64	Indicates a specific prefix.
Def	Indicates that the interface uses the default prefix.
Auto | CFG	Auto: indicates the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: indicates that the prefix is manually configured.
!Adv	Indicates that the prefix will not be advertised.

vltime	Indicates the valid lifetime of the prefix, measured in seconds.
pltime	Indicates the preferred lifetime of the prefix, measured in seconds.
L | !L	L: indicates that the on-link in the prefix is set. !L: indicates that the on-link in the prefix is not set.
A | !A	A: indicates that the auto-configure in the prefix is set. !A: indicates that the auto-configure in the prefix is not set.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Command History

Version	Description
N/A	N/A

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
vrf-name	VRF name.
verbose	Displays the neighbor details.
interface-id	Displays the neighbors of the specified interface.
ipv6-addres	Displays the neighbors of the specified IPv6 address.
static	Displays the validity status of static neighbors.

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
```

The following example displays 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	Description
IPv6 Address	Indicates the IPv6 address of the neighbor.
Linklayer Addr	Indicates the link-layer address, namely, MAC address. If it is not available, incomplete is displayed.
Interface	Indicates the interface where the neighbor is located.
State	State of the neighbor: state/H(R) The values of **STATE** are as follows: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The device is connected with the neighbor. In this state, the device takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the device takes no additional action; it only starts neighbor unreachability detection (NUD) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in the 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 (5 seconds), and 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 reaches MAX_UNICAST_SOLICIT(3). ?: indicates an unknown state. /R: indicates that the neighbor is considered as a device /H: indicates that the neighbor is considered as a host.
Age	Indicates 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 reachable time of the neighbor expires, and the neighbor waits for the triggering of NUD.
Asked	Indicates the number of the NSs that are sent to the neighbor for the resolution of the link-layer address of the neighbor.

- The following example displays the status of static neighbors.

```
Ruijie# show ipv6 neighbors static
IPv6 Address    Linklayer Addr  Interface              State
2001:1::1       00d0.f822.33ab   GigabitEthernet 0/14   ACTIVE
```

```
2001:2::2        00d0.f822.33ac   VLAN 1                INACTIVE
```

Field	Description
IPv6 Address	Indicates the IPv6 address of a static neighbor.
Linklayer Addr	Indicates the configured link-layer address, namely, MAC address.
Interface	Indicates the interface where the neighbor is located.
State	Indicates the state of the static neighbor. The values of STATE are as follows: ACTIVE: The neighbor is active. INACTIVE: The neighbor is inactive. When the IPv6 address configured for the static neighbor does not match the address configured on the interface (the IPv6 address is not in any address section of the interface or conflicts with the interface address), the static neighbor is inactive, that is, packets will not be forwarded according to the MAC address specified by the static neighbor.

Related Commands

Command	Description
ipv6 neighbor	Configures a neighbor.

Platform Description N/A

Command History

Version	Description
10.4(3)	The **vrf** *vrf-name* parameter is supported and tested.

show ipv6 neighbors statistics

Use the following command to display the statistics of IPv6 neighbors in a neighbor table.
show ipv6 neighbors [**vrf** *vrf-name*] **statistics**
Use the following command to display 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 The following example displays the statistics of global neighbors.

Examples

```
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
```

- The following example displays the statistics of all neighbors.

```
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

The command is supported on all platforms.

Command History	Version	Description
	10.4(3)	The command is added. The **vrf** *vrf-name* parameter is supported and tested.

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	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 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 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 The command is supported on all platforms.

Command History	Version	Description
	10.4(3)	The command is added.

show ipv6 route

Use this command to display the IPv6 route information.

show ipv6 route [**vrf** *vrf-name*] [**static** | **local** | **connected**]

Parameter Description	Parameter	Description
	vrf-name	VRF name.
	static	Displays the static routes.
	local	Displays the local routes.
	connected	Displays the direct routes.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the routing table.

Configuration Examples

```
Ruijie# show ipv6 route
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
 I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
L ::1/128
 via ::1, loopback 0
C fa::/64
 via ::, vlan 1
L fa::1/128
```

```
 via ::, loopback 0
C 2001::/64
 via ::, vlan 2
L 2001::1/128
 via ::, loopback 0
L fe80::/10
 via ::1, Null0
C fe80::/64
 via ::, vlan 1
L fe80::200:ff:fe00:1/128
 via ::, loopback 0
C fe80::/64
 via ::, vlan 2
```

Related Commands	Command	Description
	ipv6 route	Configures a static route.

Platform Description N/A

Command History	Version	Description
	10.4(3)	The **vrf** *vrf-name* parameter is supported and tested.

show ipv6 route summary

Use the following command to display the statistics of one IPv6 routing table.

show ipv6 route [**vrf** *vrf-name*] **summary**

Use the following command to display the statistics of all IPv6 routing tables.

show ipv6 route summary a ll

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 routing table.

```
Ruijie#show ipv6 route summary
IPv6 routing table name is Default(0) global scope - 2 entries
IPv6 routing table default maximum-paths is 32
Local           2
Connected       0
Static          0
RIP             0
OSPF            0
BGP             0
------------------------
Total           2
```

The following example displays the statistics of all routing tables.

```
Ruijie#show ipv6 route summary all
IPv6 routing table count: 2
Total
  Memory: 2000 bytes
  Entries: 20
    Local:2,Connected:2,Static:8,RIP:2,OSPF:2,ISIS:2,BGP:2

Global
  Memory: 1000 bytes
  Entries: 10
    Local:1,Connected:1,Static:4,RIP:1,OSPF:1,ISIS: 1,BGP:1

VRF1
  Memory: 1000 bytes
  Entries: 10
    Local:1,Connected:1,Static:4,RIP:1,OSPF:1,ISIS: 1,BGP:1
```

Related Commands	Command	Description
	ipv6 route	Configures a static route.

Platform Description N/A

Command History	Version	Description
	10.4(3)	The **vrf** *vrf-name* parameter is supported and tested. The **show ipv6 route summary all** command is added.

show ipv6 routers

In the IPv6 network, some neighbor routers send out RA messages. Use this command to display the neighbor routers and the RA information.

show ipv6 routers [*interface-type interface-number*]

Parameter Description	Parameter	Description
	interface-type interface-number	(Optional) Displays the RA information received by a specified interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the neighbor routers and the RA information. If no interface is specified, all the RA information received by this device will be displayed.

Configuration Examples The following example displays IPv6 routers.

```
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 sec, preferred lifetime 604800 sec
```

Related Commands

Command	Description
N/A	N/A

Platform Description The command is supported on all platforms.

Command History

Version	Description
N/A	N/A

NAT-PT Commands

clear ipv6 nat statistics

Use this command to clear NAT-PT statistics.

clear ipv6 nat statistics

Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears NAT-PT statistics.

```
Ruijie#clear ipv6 nat statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

clear ipv6 nat translations

Use this command to clear the NAT-PT translation records.

clear ipv6 nat translations { ***** | **icmp | tcp** | **udp** }

Description

Parameter	Description
*	Clears all records of NAT-PT.
icmp	Clears all records of NAT-PT for ICMP.
tcp	Clears all records of NAT-PT for TCP.
udp	Clears all records of NAT-PT for UDP.

Default N/A

Configuration

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all records of NAT-PT.

```
Ruijie#clear ipv6 nat translations *
```

The following example clears all records of NAT-PT for TCP.

```
Ruijie#clear ipv6 nat translations tcp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug ipv6 nat

Use this command to debug NAT-PT. Use the **no** form of this command to disable NAP-PT debugging.

debug ipv6 nat [**alg** | **distribute** | **event** | **memory** | **pool** | **rule**]

no debug ipv6 nat [**alg** | **distribute** | **event** | **memory** | **pool** | **rule**]

Description

Parameter	Description
alg	Enables ALG debugging for NAT-PT.
distribute	Enables distribution debugging for NAT-PT.
event	Enables event debugging for NAT-PT.
memory	Enables memory debugging for NAT-PT.
pool	Enables address pool debugging for NAT-PT.
rule	Enables rule debugging for NAT-PT.

Default Configuration N/A

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration The following example enables NAT-PT debugging.

Examples

```
Ruijie#debug ipv6 nat
```

Related Commands

Command	Description
show ipv6 nat { **memory** | **pool** | **rule** | }	Displays the information about memory, allocated address pool and rules of NAT-PT.

Platform Description

The **debug ipv6 nat distribute** command is supported on the distributed device.

ipv6 nat

Use this command to enable NAT-PT. Use the **no** form of this command to disable NAP-PT.

ipv6 nat

no ipv6 nat

Description

Parameter	Description
N/A	N/A

Default Configuration

N/A

Command Mode

Interface configuration mode.

Usage Guide

Enable the NAT-PT function on the interface.

Configuration Examples

The following example enables NAT-PT on FastEthernet 1/0.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#interface FastEthernet 1/0
Ruijie(conf-if)#ipv6 nat
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 nat prefix

Use this command to configure the IPv6 prefix for NAT-PT. Use the **no** form of this command to

remove the IPv6 prefix configuration.

ipv6 nat prefix *ipv6-prefix/prefix-length*

no ipv6 nat prefix *ipv6-prefix/prefix-length*

Description

Parameter	Description
ipv6-prefix	Indicates the global IPv6 prefix.
prefix-length	Indicates the length of global IPv6 prefix.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide There are two purposes for NAT-PT prefix configuration:

- The device compare the prefix of the destination address of the packets sent from IPv6 to IPv4 with the NAT-PT prefix, if the prefixes are matched, the packets will be processed by NAT-PT.
- For the NAT-PT enabled interface, if the source IP of the packets sent from IPv4 to IPv6 cannot be matched with the static or dynamic address mapping, the NAT-PT prefix will be used as the source IPv6 address of the packets.

Configuration Examples The following example configures the global IPv6 prefix.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat prefix 2010:3cfa::/96
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 nat service

Use this command to enable DNS/FTP ALG. Use the **no** form of this command to disable DNS/FTP ALG.

ipv6 nat service { **dns** | **ftp** }

no ipv6 nat service { **dns** | **ftp** }

Description

Parameter	Description
dns	Enables DNS ALG.
ftp	Enables FTP ALG.

Default Configuration By default, DNS ALG is disabled while FTP ALG is enabled.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables DNS ALG.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat service dns
```

The following example disables FTP ALG.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#no ipv6 nat service ftp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 nat translation

Use this command to configure the maximum entries or the protocol timeout time of NAT-PT. Use the **no** form of this command to remove the configuration.

ipv6 nat translation { **dns-timeout** *seconds* | **finrst-timeout** *seconds* | **icmp-timeout** *seconds* | **max-entries** *number* | **syn-timeout** *seconds* | **tcp-timeout** *seconds* | **timeout** *seconds* | **udp-timeout** *seconds* }

no ipv6 nat translation { **dns-timeout** | **finrst-timeout** | **icmp-timeout** | **max-entries** | **syn-timeout** | **tcp-timeout** | **timeout** | **udp-timeout** }

Description

Parameter	Description
dns-timeout *seconds*	Sets the DNS timeout. The range is from 0 to 536,870. The default value is 300. The unit is second.
finrst-timeout *seconds*	Sets the finrst timeout. The range is from 0 to 536,870. The default value is 60. The unit is second.
icmp-timeout *seconds*	Set the ICMP timeout. The range is from 0 to 536,870. The default value is 90. The unit is

	second.
number	Configures the maximum number of NAT-PT entries. The range is from 1 to 100,000, and the default value is 10,240.
syn-timeout *seconds*	Sets the SYN timeout. The range is from 0 to 536,870. The default value is 60. The unit is second.
tcp-timeout *seconds*	Sets the TCP timeout. The range is from 0 to 536,870. The default value is 86,400. The unit is second.
timeout *seconds*	Sets the timeout for other packets. The range is from 0 to 536,870. The default value is 300. The unit is second.
udp-timeout *seconds*	Sets the UDP timeout. The range is from 0 to 536,870. The default value is 300. The unit is second.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide


Note

The maximum number of NAT-PT entries are only effective for the new session. If the timeout parameter is set to 0, the session will never time out.

Configuration Examples

■ The following example configures the maximum number of NAT-PT entries to 1,000.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat translation max-extries 1000
```

The following example configures the NAT-PT timeout to 300 seconds.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat translation timeout 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 nat v4v6 pool

Use this command to configure an IPv6 address pool. Use the **no** form of this command to remove the IPv6 address pool.

ipv6 nat v4v6 pool *v6pool-name start-ipv6 end-ipv6* **prefix-length** *prefix-length*

no ipv6 nat v4v6 pool *v6pool-name*

Description

Parameter	Description
v6pool-name	Indicates the address pool name.
start-ipv6	Indicates the start IP address.
end-ipv6	Indicates the end IP address.
prefix-length	Indicates the prefix length.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide To perform NAT-PT, you need to specify the start and end IPv6 addresses.

Configuration Examples The following example configures an IPv6 address pool.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat v4v6 pool v6pool 2001:db8:0::1 2001:db8:0::10 prefix-length 64
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 nat v4v6 source

Use this command to configure the static IPv4-IPv6 address mapping. Use the **no** form of this command to remove the address mapping.

ipv6 nat v4v6 source *ipv4-address ipv6-address*

no ipv6 nat v4v6 source *ipv4-address ipv6-address*

Description

Parameter	Description
ipv4-address	Indicates the IPv4 address.
ipv6-address	Indicates the IPv6 address.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the static IPv4-IPv6 address mapping.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat v4v6 source 10.8.2.2 2012:3cfa::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 nat v4v6 source list

Use this command to configure the dynamic IPv4-IPv6 address mapping list. Use the **no** form of this command to remove the address mapping list.

ipv6 nat v4v6 source list *access-list-name* **pool** *v6pool-name*

no ipv6 nat v4v6 source list *access-list-name* **pool** *v6pool-name*

Description

Parameter	Description
access-list-name	Indicates the IPv4 ACL name.
v6pool-name	Indicates the IPv6 address pool name.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide An IPv6 ACL with the **permit** entry is required before you configure this command. The dynamic allocated IPv6 address in the address pool is used to match the packets.

Configuration Examples The following example configures the dynamic IPv4-IPv6 address mapping.

```
Ruijie#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat v4v6 source list v4-list1 pool v6pool
Ruijie(config)#ipv6 nat v4v6 pool v6pool 2010:3cfa::3 2010:3cfa::10 prefix-length 64
Ruijie(config)#access-list v4-list1 permit 192.168.10.0 0.0.0.255
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 nat v6v4 pool

Use this command to configure an IPv4 address pool. Use the **no** form of this command to remove the IPv4 address pool.

ipv6 nat v6v4 pool *v4pool-name start-ipv4 end-ipv4* **prefix-length** *prefix-length*

no ipv6 nat v6v4 pool *v4pool-name*

Description

Parameter	Description
v4pool-name	Indicates the address pool name.
start-ipv4	Indicates the start IP address.
end-ipv4	Indicates the end IP address.
prefix-length	Indicates the length of IPv4 prefix.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide To perform NAT-PT, you need to specify the start and end IPv4 addresses.

Configuration Examples The following example configures an IPv4 address pool.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat v6v4 pool v4pool 10.8.1.2 10.8.1.10 prefix-length 24
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

ipv6 nat v6v4 source

Use this command to configure the static IPv6-IPv4 address mapping. Use the **no** form of this command to remove the address mapping.

ipv6 nat v6v4 source *ipv6-address ipv4-address*

no ipv6 nat v6v4 source *ipv6-address ipv4-address*

Description

Parameter	Description
ipv6-address	Indicates the IPv6 address.
ipv4-address	Indicates the IPv4 address.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide Use this command to configure the static source IPv6-IPv4 address mapping.

Note This command is mandatory for source address mapping.

Configuration Examples The following example configures the static IPv6-IPv4 address mapping.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat v6v4 source 2012:3cfa::2 10.8.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 nat v6v4 source list

Use this command to configure the dynamic IPv6-IPv4 address mapping list. Use the **no** form of this command to remove the address mapping list.

ipv6 nat v6v4 source list *access-list-name* **pool** *v4pool-name* [**overload**]

no ipv6 nat v6v4 source list *access-list-name* **pool** *v4pool-name*

Description

Parameter	Description
access-list-name	Indicates the IPv6 ACL name.
v4pool-name	Indicates the address pool name.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide An IPv6 ACL with the **permit** entry is required before you configure this command. The dynamic allocated IPv4 address in the address pool is used to match the packets.

Configuration Examples The following example configures the dynamic IPv6-IPv4 address mapping.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat v6v4 source list v6-list1 pool v4pool
Ruijie(config)#ipv6 nat v6v4 pool v4pool 10.8.1.2 10.8.1.10 prefix-length 24
Ruijie(config)#ipv6 access-list v6-list1
Ruijie(config-ipv6-nacl)#permit ipv6 2010:3cfa::/64 any
```

The following example configures the dynamic IPv6-IPv4 address mapping.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#ipv6 nat v6v4 source list v6-list1 pool v4pool2 overload
Ruijie(config)#ipv6 nat v6v4 pool v4pool2 10.8.1.2 10.8.1.10 prefix-length 24
Ruijie(config)#ipv6 access-list v6-list2
Ruijie(config-ipv6-nacl) #permit ipv6 2010:3cfa::/64 any
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 nat memory

Use this command to display the NAT-PT memory usage.

show ipv6 nat memory

Description

Parameter	Description
N/A	N/A

Default N/A

Configuration

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the NAT-PT memory usage.

Configuration Examples The following example displays the NAT-PT memory usage.

```
Ruijie#show ipv6 nat memory
IPv6 NAT translations memory pool:
  Queue head : 0x7e1e4180, Queue tail: 0x7c3a8960, Object: 5000
  Allocate fail: 0, Supply: 0
IPv6 NAT cache mapping memory pool:
  Queue head : 0x7e20bea0, Queue tail: 0x7c32be60, Object: 5000
  Allocate fail: 0, Supply: 0
IPv6 NAT tslot memory pool:
  Queue head : 0x7c2aeea0, Queue tail: 0x7c231e60, Object: 5000
  Allocate fail: 0, Supply: 0
IPv6 NAT slab memory statistics:
  Allocated: 20013, Free: 0, Allocated bytes: 3162096, Free bytes: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 nat pool

Use this command to display NAT-PT address pools.

show ipv6 nat pool

Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays NAT-PT address pools.

```
Ruijie#show ipv6 nat pool
V4V6 POOL:
Pool name: p6_1
Pool index: 2  Rule index: 3  In use: 1  Pool type: 0x5
Total address: 241  Address using count: 0  Address round: 0
Start address: 2004:db8:1::10
End address: 2004:db8:1::100
Current address: 2004:db8:1::10

V6V4 POOL:
Pool name: p4_1
Pool index: 1  Rule index: 0  In use: 0  Pool type: 0x2
Total address: 241  Address using count: 0  Address round: 0
Start address: 23.1.1.10
End address: 23.1.1.250
Current address: 23.1.1.10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 nat rule

Use this command to display NAT-PT rules.

show ipv6 nat rule

Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays NAT-PT address pools.

```
Ruijie#show ipv6 nat pool
```

```
V4V6 POOL:
Pool name: p6_1
Pool index: 2  Rule index: 3  In use: 1  Pool type: 0x5
Total address: 241  Address using count: 0  Address round: 0
Start address: 2004:db8:1::10
End address: 2004:db8:1::100
Current address: 2004:db8:1::10

V6V4 POOL:
Pool name: p4_1
Pool index: 1  Rule index: 0  In use: 0  Pool type: 0x2
Total address: 241  Address using count: 0  Address round: 0
Start address: 23.1.1.10
End address: 23.1.1.250
Current address: 23.1.1.10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 nat statistics

Use this command to display statistics of NAT-PT rules.

show ipv6 nat statistics

Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays NAT-PT statistics.

```
Ruijie#show ipv6 nat statistics
Total rules: 7 (4 static, 3 dynamic)
NAT-PT interfaces:
```

```
FastEthernet 1/0
FastEthernet 1/1

Total translations: 0 (0 master, 0 slave, 0 map-cache, 0 tslot)
Created translations: 82,  Expired translations: 0,  Failed translations: 0
Hits: 871,  Packet unread: 0
Translated IPv4 packets: 648,  Translated IPv6 packets: 411
Forwarded IPv4 packets: 200482,  Forwarded IPv6 packets: 20814
Drop IPv4 packets: 0,  Drop IPv6 packets: 0
Ingress packets: 222355,  Egress packets: 1059,  Ingress IPv4: 201130,  Ingress IPv6: 21225
Ingress append packets: 82, Egress extract packets: 0, Failed append: 0
Prefix Hits: 411,  Prefix Misses: 0,  Local IPv4: 0,  Local IPv6: 0
Failed allocated source: 0,  Failed allocated destination: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 nat translations

Use this command to display the NAT-PT translation records.

show ipv6 nat translations [**verbose**]

Description

Parameter	Description
verbose	Displays details of NAT-PT translation.

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the NAT-PT translation records.

```
Ruijie#show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   10.6.1.1                  2001:db8::2
       ---                        ---
```

```
icmp  192.168.30.1,47          2001:db8::1:5,47
       10.6.1.1,47               2001:db8::2,47
icmp  192.168.30.1,46          2001:db8::1:5,46
       10.6.1.1,46               2001:db8::2,46
```

The following example displays the details of NAT-PT translation.

```
Ruijie#show ipv6 nat translations verbose

Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   10.6.1.1                 2001:db8::2
      ---                      ---
      create: 00:00:36, use: 00:01:36, type: static, direction: v6v4
icmp  192.168.30.1,47          2001:db8::1:5,47
       10.6.1.1,47               2001:db8::2,47
      update: 00:01:29, use: 00:00:20, type: dynamic, direction: v4v6
icmp  192.168.30.1,46          2001:db8::1:5,46
       10.6.1.1,46               2001:db8::2,46
      update: 00:01:16, use: 00:00:34, type: dynamic, direction: v4v6
icmp  192.168.30.1,48          2001:db8::1:5,48
       10.6.1.1,48               2001:db8::2,48
      update: 00:01:36, use: 00:00:13, type: dynamic, direction: v4v6
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Stateful NAT64 Configuration Commands

clear nat64 stateful statistics

Use this command to clear statistics about Stateful NAT64.

clear nat64 stateful statistics

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to clear various statistics about Stateful NAT64.

Configuration Examples The following example clears statistics about Stateful NAT64.

```
Ruijie#clear nat64 stateful statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug nat64 stateful

Use this command to enable Stateful NAT64 debugging functions. Use the **no** form of this command to disable corresponding Stateful NAT64 debugging functions.

debug nat64 stateful { **alg** | **control** | **event** | **memory** | **packet** | **pool** | **rule** | **translations**]

no debug nat64 stateful { **alg** | **control** | **event** | **memory** | **packet** | **pool** | **rule** | **translations**]

Parameter Description

Parameter	Description
alg	Enables the ALG debugging function of Stateful NAT64.
control	Enables the control plane debugging function of Stateful NAT64.
event	Enables the event debugging function of Stateful NAT64.
memory	Enables the memory debugging function of Stateful NAT64.

packet	Enables the debugging function for Stateful NAT64 forwarding.
pool	Enables the address pool management (address allocation debugging) function of Stateful NAT64.
rule	Enables the rule debugging function of Stateful NAT64.
translations	Enables the data plane translation recording function of Stateful NAT64.

Default Configuration No debugging function of Stateful NAT64 is enabled.

Command Mode Privileged EXEC mode

Usage Guide Running this command without any parameters can enable all Stateful NAT64 debugging functions.

Configuration Examples The following example enables the control plane debugging function of Stateful NAT64.

```
Ruijie#debug nat64 stateful control
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

nat64 enable

Use this command to enable the NAT64 function. Use the **no** form of this command to disable the function.

nat64 enable

no nat64 enable

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration NAT64 is disabled.

Command Mode Interface configuration mode

Usage Guide You can use this command to enable the NAT64 function or use the **no** form of this command to disable the function.

This command can be used in both Stateful and Stateless NAT64 scenarios.

Configuration Examples The following example enables the NAT64 function on the interface GigabitEthernet 1/0/0.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#interface GigabitEthernet 0/0/0
Ruijie(config-if-GigabitEthernet 0/0/0)#nat64 enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

nat64 prefix stateful

Use this command to configure a Stateful NAT64 IPv6 prefix. Use the **no** form of this command to cancel the prefix.

nat64 prefix stateful *ipv6-prefix/length* [**vrf** *vrf-name*]

no nat64 prefix stateful *ipv6-prefix/length* [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
ipv6-prefix	Specifies a Stateful NAT64 IPv6 prefix.
length	Specifies the prefix length.

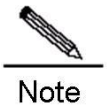
Default Configuration Global Stateful NAT64 IPv6 prefix: 64:ff9b::/96

Command Mode Global configuration mode/interface configuration mode

Usage Guide The Stateful NAT64 IPv6 prefix has the following functions:

When receiving an IPv6 network packet destined for an IPv4 network, the device compares the address prefix of the packet with the Statefull NAT64 IPv6 prefix. If the two prefixes are the same, the device delivers the packet to the NAT64 module.

When receiving an IPv4 network packet destined for an IPv6 network, the device enabled with NAT64 translates the IPv4 address of the packet into an IPv6 address using the Stateful NAT64 IPv6 prefix based on address mapping rules.



This command can be used in both global configuration mode and interface configuration mode. The prefix length can only be 32, 40, 48, 56, 64, or 96.The used VRF refers to the multi-protocol VRF, which can be used only in global configuration mode but not interface configuration mode.

Configuration Examples

The following example configures a global Stateful NAT64 prefix in global configuration mode.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 prefix stateful 2001:db8:1::/96
```

The following example configures a Stateful NAT64 prefix in interface configuration mode.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#interface gigabitethernet 1/0/0
Ruijie(config-if-GigabitEthernet 1/0/0)#nat64 prefix stateful 2001:db8:2::/96
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

nat64 service ftp

Use this command to configure the FTP ALG function. Use the **no** form of this command to cancel the configuration.

nat64 service ftp

no nat64 service ftp

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration

The FTP ALG function is enabled.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration

The following example disables the FTP ALG function.

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#no nat64 service ftp
```

Related Commands

Command	Description
show nat64 services	Displays NAT64 services.

Platform Description N/A

nat64 v4 pool

Use this command to specify an IPv4 address pool. Use the **no** form of this command to cancel the address pool.

nat64 v4 pool *pool-name start-ip-address end-ip-address*

no nat64 v4 *pool pool-name*

Parameter Description

Parameter	Description
pool-name	Specifies the name of the IPv4 address pool.
start-ip-address	Specifies the start address of the IPv4 address pool.
end-ip-address	Specifies the end address of the IPv4 address pool.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide You can use this command to specify the scope of an IPv4 address pool for NAT64. An IPv6 address can be translated into an IPv4 address in the address pool.

Configuration Examples The following example specifies an IPv4 address pool.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 v4 pool v4pool 121.165.1.1 121.165.1.254
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

nat64 v6v4 list

Use this command to configure dynamic Stateful NAT64 for translating source IPv6 addresses into source IPv4 addresses and translating destination IPv6 addresses into destination IPv4 addresses. Use the **no** form of this command to cancel the dynamic Stateful NAT64 configuration.

nat64 v6v4 list *access-list-name* **pool** *pool-name* [**overload**] [**vrf** *vrf-name*]

no nat64 v6v4 list access-list-name **pool** pool-name [**vrf** vrf-name]

Parameter Description

Parameter	Description
access-list-name	Specifies the name of an IPv6 ACL.
pool-name	Specifies the name of an IPv4 address pool.
vrf-name	Specifies a VRF name.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide You need to configure an IPv6 ACL and a permit entry. If a packet matches the ACL, an IPv4 address in the IPv4 address pool is dynamically allocated to the packet.

Configuration Examples The following example configures dynamic Stateful NAT64.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 v6v4 list nat64-acl pool v4pool
Ruijie(config)#nat64 v4 pool v4pool 121.165.1.1 121.165.1.254
Ruijie(config)#ipv6 access-list nat64-acl
Ruijie(config-ipv6-nacl)#permit ipv6 2001:db8:2::/96 any
```

The following example configures dynamic Stateful NAT64 for translating port addresses.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 v6v4 list nat64-acl pool v4pool overload
Ruijie(config)#nat64 v4 pool v4pool 121.165.1.1 121.165.1.254
Ruijie(config)#ipv6 access-list nat64-acl
Ruijie(config-ipv6-acl)#permit ipv6 2001:db8:2::/96 any
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

nat64 v6v4 static

Use this command to configure static IPv6-to-IPv4 address mapping of Stateful NAT64. Use the **no** form of this command to cancel the configuration.

nat64 v6v4 static *ipv6-address ipv4-address* [**vrf** *vrf-name*]

no nat64 v6v4 static *ipv6-address ipv4-address* [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
ipv6-address	Specifies an IPv6 address.
ipv4-address	Specifies an IPv4 address.
vrf-name	Specifies a VRF name.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide You can use this command to map a source host IPv6 address to a source IPv4 address.

Configuration Examples The following example maps the source IPv6 address to the source IPv4 address.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 v6v4 static 2001:db8:1::fffe 209.165.201.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 stateful debug-buf

Use this command to display the debugging buffer.

show nat64 stateful debug-buf

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to display information about the debugging buffer. Before using this command, enable the related debugging command.

Configuration Examples The following example displays information about the debugging buffer.

```
Ruijie#show nat64 stateful debug-buf
```

Related Commands

Command	Description
debug nat64 stateful alg	Enables the AGL debugging function of Stateful NAT64.
debug nat64 stateful event	Enables the event debugging function of Stateful NAT64.
debug nat64 stateful memory	Enables the memory debugging function of Stateful NAT64.
debug nat64 stateful packet	Enables the data plane debugging function of Stateful NAT64.
debug nat64 stateful pool	Enables the address pool debugging function of Stateful NAT64.
debug nat64 stateful rule	Enables the translation rule debugging function of Stateful NAT64.
debug nat64 stateful translations	Enables the translation recording function of Stateful NAT64.

Platform Description N/A

show nat64 mappings dynamic

Use this command to display dynamic NAT64 mapping information.

show nat64 mappings dynamic

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to display dynamic NAT64 mapping information.

Configuration Examples The following example displays dynamic NAT64 mapping information.

```
Ruijie#show nat64 mappings dynamic
Rule index: 8,  Rule type: 0x2,  Create: 02:57:29,  Update: 02:57:33
Rule use count: 0,  Status: inactive
ACL type: 2,  ACL id: 3900,  Pool id: 0
ACL: v6_acl,  Pool: v4_pool
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 mappings static

Use this command to display static NAT64 mapping information.

show nat64 mappings static

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays static NAT64 mapping information.

```
Ruijie#show nat64 mappings static
Rule index: 12,  Rule type: 0x1,  Create: 03:06:25,  Update: 03:06:25
Rule use count: 0,  Status: active
V6V4 Mapping: 3001::1 => 1.1.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 memory

Use this command to display NAT64 memory utilization.

show nat64 memory

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays NAT64 memory utilization.

```
Ruijie#show nat64 memory
NAT64 translations memory pool:
  Queue head : 0x7e1e4180, Queue tail: 0x7c3a8960, Object: 5000
  Allocate fail: 0, Supply: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 pools

Use this command to display the configured NAT64 address pool.

show nat64 pools

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configured NAT64 address pool.

```
Ruijie#show nat64 pools
V4 POOL:
Pool name: v4pool
Pool index: 1  Rule index: 0  In use: 0  Pool type: 0x2
Total address: 241  Address using count: 0  Address round: 0
Start address: 23.1.1.10
End address: 23.1.1.250
Current address: 23.1.1.10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 prefix stateful

Use this command to display all configured Stateful NAT64 IPv6 prefixes.

show nat64 prefix stateful [**interfaces**]

Parameter Description

Parameter	Description
interfaces	Specifies all interfaces.

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to display all Stateful NAT64 IPv6 prefixes configured in global and interface configuration modes.

Configuration Examples The following example displays all configured Stateful NAT64 IPv6 prefixes.

```
Ruijie#show nat64 prefix stateful interfaces

Interface              NAT64-Enable      Pref-Enable      Prefix
prefix-length
GigabitEthernet1/0/0   TRUE              TRUE             2001:db8:1::       96
GigabitEthernet1/0/1   TRUE              TRUE             2001:db8:2::       96
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 services

Use this command to display NAT64 ALG-related information.

show nat64 services

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode You can use this command to display NAT64 ALG-related information.

Usage Guide N/A

Configuration Examples The following example displays NAT64 ALG-related information.

```
Ruijie#show nat64 services
ALG specific:
ALG type: 0x1,  ALG switch: 0x1,  Proto: 6,  Port: 21
IPv4 procedure: 0xabcf70,  IPv6 procedure: 0xabc940

ALG type: 0x2,  ALG switch: 0x1,  Proto: 6,  Port: 80
IPv4 procedure: 0xabdce0,  IPv6 procedure: 0xabd508
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 stateful statistics

Use this command to display statistics about Stateful NAT64.

show nat64 stateful statistics

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays statistics about Stateful NAT64.

```
Total rules: 7 (4 static, 3 dynamic)
NAT64 interfaces:
  Gigabitethernet 1/0/0
Gigabitethernet 1/0/1

  Total translations: 0
  Created translations: 82,  Expired translations: 0,  Failed translations: 0
  Hits: 871,  Packet unread: 0
  Translated IPv4 packets: 648,  Translated IPv6 packets: 411
  Forwarded IPv4 packets: 200482,  Forwarded IPv6 packets: 20814
  Drop IPv4 packets: 0,  Drop IPv6 packets: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 translations

Use this command to display NAT64 records.

show nat64 translations

Parameter Description

Parameter	Description
N/A	N/A

Default N/A

Configuration

Command Mode Privileged EXEC mode

Usage Guide The RSR77 series router has separate NAT64 records on each line card. You can specify a line card whose NAT64 records are displayed.

Configuration Examples The following example displays NAT64 records on the line card 4/1.

```
Ruijie#show nat64 translations slot 4/1
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
icmp  192.168.30.1,47          2001:db8::1:5,47
      10.6.1.1,47              2001:db8::2,47
icmp  192.168.30.1,46          2001:db8::1:5,46
      10.6.1.1,46              2001:db8::2,46
```

Related Commands

Command	Description
N/A	N/A

Platform Description The **show nat64 translations slot** *slotnum* command is supported only by the RSR77.

Stateless NAT64 Configuration Commands

clear nat64 stateless statistics

Use this command to clears statistics about Stateless NAT64.

clear nat64 stateless statistics

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to clear various statistics about Stateless NAT64.

Configuration Examples The following example clears statistics about Stateless NAT64.

```
Ruijie#clear nat64 stateless statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug nat64 stateless

Use this command to enable Stateless NAT64 debugging functions. Use the **no** form of this command to disable Stateless NAT64 debugging functions.

debug nat64 stateless { control | **packet]**

no debug nat64 stateless { **control | packet]**

Parameter Description

Parameter	Description
control	Enables the control plane debugging function of Stateless NAT64.
packet	Enables the data plane debugging function of Stateless NAT64.

Default Configuration No debugging function of Stateless NAT64 is enabled.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example enables the statistics function of Stateless NAT64.

```
Ruijie#debug nat64 stateless packet
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

nat64 enable

Use this command to enable NAT64 on an interface. Use the **no** form of this command to disable NAT64 from the interface.

nat64 enable

no nat64 enable

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration NAT64 is disabled.

Command Mode Interface configuration mode

Usage Guide You can use this command to enable the NAT64 function or use the **no** form of this command to disable the function.

Note This command can be used in both Stateful and Stateless NAT64 scenarios.

Configuration Examples The following example enables the NAT64 function on the interface GigabitEthernet 1/0/0.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#interface GigabitEthernet 1/0/0
Ruijie(config-if-GigabitEthernet 1/0/0)#nat64 enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

nat64 prefix stateless

Use this command to configure a Stateless NAT64 IPv6 prefix. Use the **no** form of this command to cancel the prefix.

nat64 prefix stateless *ipv6-prefix/length* [**vrf** *vrf-name*]

no nat64 prefix stateless *ipv6-prefix/length* [**vrf** *vrf-name*]

Parameter Description	Parameter	Description
	ipv6-prefix	Specifies a Stateless NAT64 IPv6 prefix.
	length	Specifies the prefix length.
	vrf-name	Specifies a VRF name.

Default Configuration N/A

Command Mode Global configuration mode/interface configuration mode

Usage Guide The Stateless NAT64 IPv6 prefix hast the following functions:

When receiving an IPv6 network packet destined for an IPv4 network, the device compares the destination address prefix of the packet with the Stateless NAT64 IPv6 prefix. If the two prefixes are the same, the device delivers the packet to the NAT64 module. According to translation rules, the IPv4 address translated from the source IPv6 address is extracted from the IPv6 address.

When receiving an IPv4 network packet destined for an IPv6 network, the device enabled with NAT64 translates the IPv4 address of the packet into an IPv6 address using the Stateful NAT64 IPv6 prefix based on address mapping rules.

Note

This command can be used in both global configuration mode and interface configuration mode. The prefix length can only be 32, 40, 48, 56, 64, or 96. The used VRF refers to the multi-protocol VRF, which can be used only in global configuration mode but not interface configuration mode.

Configuration Examples The following example configures a global Stateless NAT64 IPv6 prefix.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 prefix stateless 2001:db8:1::/32
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

nat64 prefix stateless v4v6

Use this command to configure a Stateless NAT64 IPv6 prefix for IPv4-to-IPv6 address translation. Use the **no** form of this command to cancel the prefix.

nat64 prefix stateless v4v6 *ipv6-prefix/prefix-length* [**vrf** *vrf-name*]

no nat64 prefix stateless v4v6 *ipv6-prefix/prefix-length* [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
ipv6-prefix	Specifies an IPv6 prefix.
prefix-length	Specifies the prefix length.
vrf-name	Specifies a VRF name.

Default Configuration N/A

Command Mode Global configuration mode

Usage Guide You can use this command to obtain translatable IPv6 addresses for IPv4 hosts. Stateless NAT64 can map an IPv4 host address to an IPv6 address.

Note The prefix length can only be 32, 40, 48, 56, 64, or 96.

Configuration Examples The following example configures a Stateless NAT64 IPv6 prefix for IPv4-to-IPv6 address translation.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 prefix stateless v4v6 2001:db8:2::/96
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

nat64 prefix stateless v6v4

Use this command to configure a Stateless NAT64 IPv6 prefix for IPv6-to-IPv4 address translation. Use the **no** form of this command to cancel the prefix.

nat64 prefix stateless v6v4 *ipv6-prefix/prefix-length*

no nat64 prefix stateless v6v4 *ipv6-prefix/prefix-length*

Parameter Description

Parameter	Description
ipv6-prefix	Specifies an IPv6 prefix.
prefix-length	Specifies the prefix length.

Default Configuration N/A

Command Mode Interface configuration mode

Usage Guide You can use this command to map an IPv6 host address to an IPv4 address in Stateless NAT64 scenario.

Note The prefix length can only be 32, 40, 48, 56, 64, or 96.

Configuration Examples The following example configures a Stateless NAT64 IPv6 prefix for IPv6-to-IPv4 address translation.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#nat64 prefix stateless v6v4 2001:db8:0:1::/96
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

nat64 route

Use this command to configure a route which starts from an IPv4 network and is destined for a specific IPv6 interface for Stateless NAT64. Use the **no** form of this command to cancel the route.

nat64 route *ipv4-prefix/mask interface-type interface-number* [**vrf** *vrf-name*]

no nat64 route *ipv4-prefix/mask interface-type interface-number* [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
ipv4-prefix	Specifies an IPv4 address prefix.
mask	Specifies an IPv4 address mask.
interface-type	Specifies an interface type.
interface-number	Specifies an interface number.
vrf-name	Specifies a VRF name.

Default Configuration

N/A

Command Mode

Global configuration mode

Usage Guide

You can use this command to configure a route which starts from an IPv4 network segment and is destined for a specific IPv6 interface. The network segment address is translated on the specific IPv6 interface.

Configuration Examples

The following example configures a route which starts from an IPv4 network segment and is destined for a specific IPv6 interface.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Ruijie(config)#nat64 route 203.0.113.0/24 gigabitethernet 0/0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show nat64 stateless debug-buf

Use this command to display the debugging buffer of Stateless NAT64.

show nat64 stateless debug-buf

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to display information about the debugging buffer. Before using this command, enable the related debugging command.

Configuration Examples The following example displays information about the debugging buffer.

```
Ruijie#show nat64 stateless debug-buf
-----------------------------------------------------
         display the NAT64 stateless log information
total: 65536Byte  used: 0Byte  percentage: 0%
-----------------------------------------------------
there is no NAT64 stateless log information
NAT64_SL_DBGD:FUNC:nat64_stateless_ipv4_in       line:63   :IPV4:PKT INGRESS:**:sip
32.1.1.2,dip 20.1.1.2,pro 1,fid 7663504,num 92992074.
NAT64_SL_DBGD:FUNC:nat64_stateless_ipv4_in       line:79   :IPV4:flow_event 1,flow_nat64
1.
NAT64_SL_DBGD:FUNC:nat64_stateless_ipv6_in       line:239  :IPV6:PKT INGRESS:##:sip
3001::1401:102,dip 1001::2001:102,fid 13889401,num 1355078.
NAT64_SL_DBGD:FUNC:nat64_stateless_ipv6_in       line:255  :IPV6:flow_event 1,flow_nat64
1.
-----------------------------------------------------
```

Related Commands

Command	Description
debug nat64 stateless packet	Enables the data plane debugging function of Stateless NAT64.

Platform Description N/A

show nat64 prefix stateless

Use this command to display all configured Stateless NAT64 IPv6 prefixes.

show nat64 prefix stateless [**interfaces**]

Parameter Description

Parameter	Description

interfaces	Specifies interface prefixes.

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to display all Stateless NAT64 IPv6 prefixes configured in global and interface configuration modes.

Configuration Examples The following example displays all Stateless NAT64 IPv6 prefixes configured in interface configuration mode.

```
Ruijie#show nat64 prefix stateless interfaces
NAT64 Stateless Prefixes

Interface       NAT64-Enable   Pref-Enable   Prefix              v6v4
Gi1/0/0         TRUE           TRUE          3001::/96           TRUE
Gi1/0/1         TRUE           TRUE          5001::/96           FALSE
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show nat64 stateless statistics

Use this command to display statistics about Stateless NAT64.

show nat64 stateless statistics

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command to display all statistics about Stateless NAT64.

Configuration The following example displays all statistics about Stateless NAT64.

Examples

```
Ruijie#show nat64 stateless statistics
NAT64 Stateless Global stats:
    Created Packets translation (IPv4 -> IPv6): 0.
    Created Packets translation (IPv6 -> IPv4): 0.
    Packets droped in IPv4: 0.
    Packets droped in IPv6: 0.

NAT64 Stateless Interface stats:
    Vl10:
       Created Packets translation (IPv4 -> IPv6): 4.
       Created Packets translation (IPv6 -> IPv4): 0.

    Gi0/1:
       Created Packets translation (IPv4 -> IPv6): 0.
       Created Packets translation (IPv6 -> IPv4): 1.

    Gi0/0:
       Created Packets translation (IPv4 -> IPv6): 0.
        Created Packets translation (IPv6 -> IPv4): 0.
```

Related Commands

Command	Description
clear nat64 stateless statistics	Clears statistics about Stateless NAT64.

Platform Description

N/A