Ruijie RG-IS2700G Series Switches

RGOS Command Reference, Release 10.4(3b16)T2

Copyright Statement

Exemption Statement

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

Preface

Thank you for using our products. This manual matches the RGOS Release 10.4(3b16)T2.

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.

System Configuration

1. CLI Authorization Configuration Commands
2. Basic Configuration Management
3. HTTP Service Configuration Commands
4. UPGRADE Configuration Commands
5. LINE Configuration Commands
6. File System Configuration Commands
7. Configuration Commands of Configuration File Management
8. CPU-LOG Configuration Commands
9. Memory Commands
10. Syslog Configuration Commands
11. Cluster Management Configuration Commands
12. Redundancy Configuration Commands
13. SRM Configuration Commands
14. Hardware Entry Capacity Commands

CLI Authorization Configuration Commands

alias

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

alias *mode command-alias original-command*

no alias *mode command-alias*

Parameter Description

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

Defaults

Some commands in EXEC mode have default alias.

Command Mode

Global configuration mode.

Usage Guide

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

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

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

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

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

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

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

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

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

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

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

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

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

```
Ruijie# s?
show  start-chat  start-terminal-service
```

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

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

The above help information lists the parameters of **ip address** and shows the actual command name.

You must enter an entire alias; otherwise it cannot be recognized.

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

Configuration Examples

#In global configuration mode, use def-route to represent the default route setting of ip route 0.0.0.0 0.0.0.0 192.168.1.1:

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

Related Commands

Command	Description
show aliases	Shows the aliases settings.

Platform Description

N/A

privilege

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

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

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

Parameter Description

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

Defaults

N/A.

Command Mode

Global configuration mode.

Usage Guide

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

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

Configuration Examples

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

```
Ruijie(config)#enable secret level 1 0 test
Ruijie(config)#privilege exec level 1 reload
After the above setting, you can access the CLI window as level-1 user to use
the reload command:
Ruijie>reload ?
LINE   Reason for reload
<cr>
```

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

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

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

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

Related Commands

Command	Description
enable secret	Sets the CLI-level password.

Platform Description

N/A.

show aliases

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

show aliases [*mode*]

Parameter Description

Parameter	Description
mode	Mode of the command represented by the alias.

Defaults

N/A.

Command Mode

EXEC mode.

Usage Guide

Show the configuration of all aliases if no command mode is input.

Configuration Examples

#Show the command alias in EXEC mode:

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

Related Commands

Command	Description

alias	Sets a command alias.

Platform Description N/A.

Basic Configuration Management

banner login

To configure the login banner, execute the **banner login** command in the global configuration mode. You can use the **no banner login** command to remove the configuration.

banner login *c message c*

Parameter Description

Parameter	Description
c	Separator of the message of logging banner. Delimiters are not allowed in the MOTD.
message	Contents of login banner

Defaults -

Command Mode Global configuration mode.

Usage Guide This command sets the logging banner message, which is displayed upon login. All characters behind the terminating symbol will be discarded by the system.

Configuration Examples The following example shows the configuration of logging banner:

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

Related Commands

Command	Description
-	-

Platform Description -

banner motd

To set the Message-of-the-Day (MOTD), run the **banner motd** command in the 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 -

Command Mode Global configuration mode.

Usage Guide

This command sets the MOTD, which is displayed upon login. The letters entered after 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

-

clock set

To configure system clock manually, execute one of the two formats of the privileged user command clock set:

clock set *hh:mm:ss month day year*

Parameter Description

Parameter	Description
hh:mm:ss	Current time, in the format of Hour (24-hour): Minute: Second
day	Date (1-31) of month
month	Month (1-12) OF year
year	Year (1993-2035), abbreviation is not allowed.

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to set the system time to facilitate the management.

For devices without hardware clock, the time set by the clock set command takes effect for only the current setting. Once the device powers off, the manually set time becomes invalid.

Configuration Examples

The example below 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	Show current clock.

Platform Description

N/A

clock update-calendar

This command is used to update the value of the hardware clock of the system to that of the current software clock.

clock update-calendar

Parameter Description

Parameter	Description

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

Some platforms use hardware clock to complement software clock. Since battery enables hardware clock to run continuously, even though the device is closed or restarts, hardware clock still runs.

If hardware clock and software clock are asynchronous, then software clock is more accurate. Execute clock update-calendar command to copy date and time of software clock to hardware clock.

Configuration Examples

The example below copies the current time and date of software clock to hardware clock:

```
Ruijie# clock update-calendar
```

Related Commands

Command	Description

Platform Description

N/A

disable

To exit from privileged user mode to normal user mode or lower the privilege level, execute the privileged user command disable.

disable [*privilege-level*]

Parameter Description

Parameter	Description
privilege-level	Privilege level

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to return to user mode from privileged EXEC mode. If a privilege level is added, the current privilege level will be lowered to the specified level.

Caution The privilege level following the disable command must be lower than the current level.

Configuration Examples

The example below lowers the current privilege level of the device down to level 10:

```
Ruijie# disable 10
```

Related Commands

Command	Description
enable	From user mode enter to the privileged EXEC mode or log on the higher level of authority.

Platform Description

-

enable

To enter into the privileged user mode, execute the normal user configuration command **enable**.

enable

Parameter Description

Parameter	Description

Defaults

-

Command Mode

-

Usage Guide

-

Configuration Examples

-

Related Commands

Command	Description
-	-

Platform Description

-

enable password

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

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

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

Parameter Description

Parameter	Description
password	Password for user to enter into the EXEC configuration layer
level	User's level.
0|7	Password encryption type, "0" for no encryption, "7" for simple encryption
encrypted-password	Password text.

Defaults

-

Command Mode

Global configuration mode.

Usage Guide

No encryption is required in general. The encryption type is required generally when the password that has been encrypted with the command for the device are to be copies and pasted.

The effective password is defined as below:

Consists of 1 ~ 26 letter in upper/lower case and numerals

Leading spaces are allowed but ignored. Spaces in between or at the end are regarded as part of the password.

Caution

If an encryption type is specified and then a plaintext password is entered, it is impossible to enter into the privileged EXEC mode. A lost password that has been encrypted with any method cannot be restored. The only way is to reconfigure the device password.

Configuration Examples

The example below configures the password as pw10:

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

Related Commands

Command	Description
enable secret	Set the security password

Platform Description

-

enable secret

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

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

no enable secret [**level** *level*]

Parameter Description

Parameter	Description
secret	Password for user to enter into 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

-

Command Mode

Global configuration mode.

Usage Guide

The password falls into "password" and "security" passwords. The "password" is simple encryption password, which can be set only for level 15. The "security" means the security encryption password, which can be set for level 0 ~ 15. If the two kinds of passwords exist in the system at the same time, the "password" type password will not take effect. If a "password" type password is set for a level other than 15, an alert is provided and the password is automatically converted into the "security" password. If "password" type password is set for level 15 and the same as the "security" password, an alert is provided. The password must be saved in encrypted manner, with simple encryption for the "password" type password and security encryption for the "security" type password.

Configuration Examples

The example below configures the security password as pw10:

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

Related Commands

Command	Description
enable password	Set passwords for different privilege levels.

Platform Description

-

enable service

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

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

Parameter Description

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

	enabled at the same time.

Defaults

-

Command Mode

Global configuration mode.

Usage Guide

This command is used to enable the specified service. Use the no enable service command to disable the specified service.

Caution

The enable service web-server command is followed with three optional key words: http, https and all. If no key word or the key word all follows the command when it is used, http and https services are enabled concurrently. If the key word http follows the command, only http service is enabled. If the key word https follows the command, only https service is enabled.

Configuration Examples

The example below enables the SSH Server:

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

Related Commands

Command	Description
show service	View the service status of the current system.

Platform Description

-

exec-timeout

To configure the connection timeout to this equipment in the LINE, use the **exec-timeout** command. Once the connection timeout in the LINE is cancelled by the **no exec-timeout** command, the connection will never be timeout.

exec-timeout *minutes* [*seconds*]

no exec-timeout

Parameter Description

Parameter	Description
minutes	The minutes of specified timeout.
seconds	(optional parameter) The seconds of specified timeout.

Defaults

The default timeout is 10min.

Command Mode

Line configuration mode.

Usage Guide

If there is no input/output information for this connection within specified time, this connection will be interrupted, and this LINE will be restored to the free status.

Configuration

The example below specifies the connection timeout is 5’30“.

Examples

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

Related Commands

Command	Description

Platform Description

-

execute

To execute the commands in the batch files, use the privileged EXEC mode command **execute**.

execute [**flash:**] *filename*

Parameter Description

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

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

This command is used to execute the commands in the batch files.

Users could self-specify the filename and content of the batch file. In general, after finishing editting the batch files on the user PC , the files are transmit to the Flash of the device through the TFTP. The content of batch files completely imitates the user entering, so the content should be edited in order of CLI command configuration. Besides, for some interactive commands , the response message should be pre-wrote into the batch files to ensure the commands can be normally executed.

Caution

The size of the batch file shall not exceed 128K, otherwise the execution of batch files may fail. For the over-sized batch files, you can divide them into several small files with size less than 128K to complete the execution.

Configuration Examples

The example below executes the batch file line_rcms_script.text ,which is used to enable the reverse Telnet function for all asynchronous Interfaces, and whose contents are as follows:

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

The execution result is as below:

```
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

Platform Description

-

hostname

To specify or modify the hostname of the device, execute the global configuration command **hostname.**

hostname *name*

Parameter Description

Parameter	Description
name	Device hostname, the string, numeral or hyphen are supported only. The maximum length is 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 in the dialup and CHAP authentication.

Configuration Examples

The example below configures the hostname of the device as BeiJingAgenda:

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

Related Commands

Command	Description

Platform Description

-

ip http authentication

When using the Http Server, it needs to perform the logon authentication to enter the Web page. Use this command to set the mode of Web logon authentication.

ip http authentication {enable | local }

Parameter Description

Keyword	Description
enable	Use the password set by the **enable password** or **enable secret**, the password must be of the level15.
local	Use the username and password set by the local username command. The user must bind to the privilege of level15.

Defaults

By default, the system uses enable authentication.

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 example below sets the mode of Web logon authentication as local:

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

Related Commands

Command	Description
enable service	Enable or disable the specified service.

Platform Description

-

ip http port

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

ip http port *number*

Parameter Description

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

Defaults

80

Command Mode

Global configuration mode.

Usage Guide

This command is used to set the port of the HTTP service. Use the no ip http port command to restore it to the default setting.

Configuration Examples

The example below set the port of the HTTP service as 8080:

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

Related commands

Command	Description
enable service	Enable or disable the specified service.

ip http source-port

This command is used to configure the port for HTTPS services in the global configuration mode.

ip http source-port *number*

Parameter Description

Parameter	Description
number	Configure the port for HTTPS services, and the default value is 443.

Defaults

443

Command Mode

Global configuration mode.

Usage Guide

This command is used to configure the port for HTTPS services. The no form of this command is used to restore the default port configuration.

Configuration Examples

The example below sets the port for HTTPS services as 4443.

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

Related Commands

Command	Description
enable service	Enable or disable the specified service.
show web-server status	Show the status of the web server.

Platform Description

-

ip telnet source-interface

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

ip telnet source-interface *interface-name*

Parameter Description

Keyword	Description
interface-name	Name of the specified interface

Defaults

-

Command Mode

Global configuration mode.

Usage Guide

This command is used to specify the IP address of one interface as the source address for the global Telnet connetction. When using the telnet command to log in a Telnet server, if no source interface or source address is specified for this connnetcion, the global setting is used.Use the no ip telnet source-interface command to restore it to the default setting.

Configuration Examples

The example below specifies the IP address of the interface *Loopback1* as the source address for the global Telnet connection.

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

Related Commands

Command	Description
telnet	log in a Telnet server

Platform Description

-

lock

To set a temporary password at the terminal, execute the EXEC mode command **lock**.

lock

Parameter Description

Parameter	Description

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

You can lock the terminal interface but maintain the continuity of session, to prevent it from being accessed by setting the temporary password. The terminal interface can be locked by the steps below:

- Enter the lock command, and the system will prompt you to enter the password:
- Enter the password, which may be any string.The system will prompt you to confirm the entered password, and then clear the screen as well as show the "Locked" information.
- To enter into the terminal, enter the set temporary password.

To use the terminal locked function at the terminal, execute the lockable command in the line configuration mode, and enable the characteristic to support the terminal lock in corresponding line.

Configuration Examples

The example below locks a terminal interface:

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

Related Commands

Command	Description
lockable	Set to support the terminal lock function in the line.

Platform Description

-

lockable

To support the use of the **lock** command at the terminal, execute the **lockable** command in the line configuration mode. The terminal doesn't support the **lock** command, by default.Use the **no** command to cancel the setting.

lockable
no lockable

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Line configuration mode.

Usage Guide

This command is used to support the terminal lock function in corresponding line. To lock the terminal, execute the lock command in the EXEC mode.

Configuration Examples

The example below enables the terminal lock function at the console port and locks the console:

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

Related Commands

Command	Description
lock	Lock the terminal.

Platform Description

-

login

In case the AAA is disabled, to enable simple logon password authentication on the interface, execute the interface configuration command **login**. The **no** form of this command is used to delete the line logon password authentication.

login

no login

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Line configuration mode.

Usage Guide If the AAA security server is not enabled, this command is used for the simple password authentication at logon. The password here is the one configured for VTY or console interface.

Configuration Examples The example below shows how to set the logon 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	Configure the line logon password

Platform Description -

login authentication

In case the AAA is enabled, the authentication with the AAA server must be performed for logon. Use this command to associate logon authentication method list. The **no** form of this command is used to delete the logon authentication method 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 available

Defaults -

Command Mode Line configuration mode.

Usage Guide If the AAA security server is enabled, this command is used for the logon authentication with the specified method list.

Configuration Examples

The example below shows how to associate method list on VTY and perform logon authentication with radius.

```
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	Enable the AAA security service
aaa authentication login	Configure the logon authentication method list

Platform Description -

login local

In case the AAA is disabled, to enable local user authentication on the interface, execute the interface configuration command **login local**. The **no** form of this command is used to delete the line local user authentication.

login local

no login local

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Line configuration mode.

Usage Guide If the AAA security server is not enabled, this command is used for the local user authentication at logon. The user here means the one configured with the username command.

Configuration Examples

The example below shows how to set the 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	Configure the local user information.

Platform Description

-

password

To configure the password for line logon, execute the line configuration command **password**. The **no** form of this command is used to delete the line logon password.

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

no password

Parameter Description

Parameter	Description
password	Password for line of remote user
0|7	Password encryption type, "0" for no encryption, "7" for simple encryption
encrypted-password	Password text

Defaults

-

Command Mode

Line configuration mode.

Usage Guide

This command is used to configure the authentication password for the line logon of remote user.

Configuration Examples

The example below configures the line logon password as "red":

```
Ruijie(config)# line  vty 0
Ruijie(config-line)# password red
```

Related Commands

Command	Description
login	From user mode enter to the privileged EXEC mode or log on the higher level of authority.

Platform Description

-

password policy

Use the **password policy** command to configure password safety policy. The **no** form of this command is used to delete the password safety policy.

password policy {**min-size** *length* | **strong** | **no-repeat-times** *times* | **life-cycle** *days* }

no password { **min-size** | **strong** | **no-repeat-times** | **life-cycle** }

Parameter Description

Parameter	Description
min-size	It sets the minimum length of the password.
length	It specifies the minimum length of the password.
strong	It sets strong password check.
no-repeat-times	It restricts using the passwords configured in recent times repeatedly.
times	It specifies the passwords configured lately.
life-cycle	It configures life cycle for the password.
days	It specifies the life cycle of the password in days.

Defaults -

Command Mode Global configuration mode

Usage Guide This command is used to configure safety policy check for local passwords.

Configuration Examples

Example 1 configures the minimum length of the password to 8.

```
Ruijie(config)# password policy min-size 8
```

Example 2 configures strong password check.

```
Ruijie(config)# password policy strong
```

Example 3 restricts using the passwords configured in the last five times repeatedly.

```
Ruijie(config)# password policy no-repeat-times 5
```

Example 4 configures the life cycle of the password to 90 days.

```
Ruijie(config)# password policy life-cycle 90
```

Related Commands

Command	Description
-	-

Platform Description -

privilege mode

Please refer to the *chapter of configure CLI authorization commands.*

Parameter Description

Parameter	Description
-	-

Defaults Please refer to the chapter of *configure CLI authorization commands.*

Command Mode Please refer to the chapter of *configure CLI authorization commands.*

Usage Guide Please refer to the chapter of *configure CLI authorization commands.*

Configuration Examples Please refer to the chapter of *configure CLI authorization commands.*

Related Commands

Command	Description
-	-

Platform Description -

prompt

To set the **prompt** command, run the **prompt** command in the 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. The maximum length is 32 letters.

Defaults -

Command Mode Global configuration mode.

Usage Guide If you have not set the prompt string, the prompt string is the system name, which varies with the system name. The prompt command is valid only in the EXEC mode.

Configuration Examples Set the prompt string to RGOS:

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

Related Commands

Command	Description
-	-

Platform Description -

reload

To restart the device system, execute the privileged user command reload.

reload [*text* | **in** [*hh:*] *mm* [*text*] | **at** *hh:mm* [*month day year*] [*text*] | **cancel**]

Parameter Description

Parameter	Description
text	Cause to restart, 1-255 bytes
in *mmm hh:mm*	The system is restarted after specified time interval.
at *hh:mm*	The system is restarted at the specified time. Up to 200 days is supported
month	Month in the range January to December
day	Date in the range 1 to 31
year	Year in the range 1993 to 2035. The abbreviation is not allowed.
cancel	Cancel scheduled restart.

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

This command is used to restart the device at specified time, which may facilitate the management.

Configuration Examples

Example 1 configures to restart the system in 10 minutes.

```
Ruijie# reload in 10
Router will reload in 600 seconds
```

Related Commands

Command	Description
-	-

Platform Description

-

service password-encryption

To encrypt the password, execute this command. The **no** form of this command restores to the default value, but the password in cipher text cannot be restored to plain text.

service password-encryption

Parameter Description

Parameter	Description
-	-

Command Mode

Global configuration mode.

Usage Guide

Use the service password-encryption command to control. This command is disabled by default. Various passwords are displayed in form of plain text, unless it is directly configured in cipher text form. After you execute the service password-encryption and show running or write command to save the configuration, the password transforms into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.

Configuration Examples

The example below encrypts the password:

```
Ruijie(config)# service password-encryption
```

Related Commands

Command	Description
enable password	Set passwords of different privileges.

Platform Description

-

session-timeout

To configure the session timeout for the remote terminal established in current LINE, use the **session-timeout** command. When the session timeout for the remote terminal in the LINE is cancelled, the session will never be timeout.

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

no session-timeout

Parameter Description

Parameter	Description
minutes	The minutes of specified timeout.
output	Regard data output as the input to determine whether timeouts.

Defaults

The default timeout is 0 min.

Command Mode

LINE configuration mode.

Usage Guide

If there is no input/output information for the session to the remote terminal established in current LINE within specified time, this connection will be interrupted, and this LINE will be restored to the free status.

Configuration Examples

The example below specifies the timeout of session is 5 minutes.

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

Related Commands

Command	Description
-	-

Platform Description -

show clock

To view the system time, execute the privileged user command show clock.

show clock

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Privileged EXEC mode

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

Configuration Examples

The example below is an execution result of the show clock command:

```
Ruijie# show clock
clock: 2003-3-17 10:27:21
```

Related Commands

Command	Description
clock set	Set the system clock.

Platform Description -

show line

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

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

Parameter Description

Parameter	Description
console	Show the configuration of a console line.
aux	View the configuration of an aux line.
vty	Show the configuration of a vty line.
line-num	Number of the line

Command Mode Privileged EXEC mode.

Usage Guide This command shows the configuration information of a line.

Configuration Examples

The following example shows the configuration of console port:

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

Related Commands

Command	Description
-	-

Platform Description

-

show mainfile

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

show mainfile

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged EXEC mode

Usage Guide

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

Configuration Examples

Ruijie# show mainfile

MainFile name: /rgos.bin

Related Commands

Command	Description
N/A	N/A

Platform description

N/A

show reload

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

show reload

Parameter Description

Parameter	Description
-	-

Defaults

-

Command mode

Privileged EXEC mode.

Usage Guide

Use this command 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
-	-

Platform Description

-

show running-config

To show the configuration information current device system is running, execute the privileged user command show running-config.

show running-config

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide -

Configuration Examples -

Related Commands

Command	Description
-	-

Platform Description -

show startup-config

To view the configuration of device stored in the Non Volatile Random Access Memory (NVRAM), execute the privileged user command show startup-config.

startup-config

show startup-config

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Privileged EXEC mode.

Usage Guide

The configuration of device stored in the NVRAM is that executed when the device is startup.

On devices that do not support the boot config command, startup-config indicates the configuration stored in the default configuration file "/config.text" in built-in flash of devices.

On devices that use the boot config command to specify the startup configuration file, the configuration indicated by startup-config complies with the following rules:

- If the name of the startup configuration file is configured by the boot config command and the file exists, startup-config indicates the configuration stored in the configuration file that specified by the boot config command.
- If the configuration file specified by the boot config command does not exist or the name of the startup configuration file is not configured by the boot config command, startup-config indicates the configuration stored in the default configuration file "/config.text" in built-in flash of devices.

Configuration Examples -

Related

Command	Description

Commands

boot config	Set the name of the startup configuration file of the device.

Platform Description

-

show this

Use the **show this** command in the current mode to view effective configuration of the system in the current mode.

show this

Parameter Description

Parameter	Description
-	-

Defaults

None

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to view effective configuration in the current mode.

Configuration Examples

The following example views effective configuration of interface fastEthernet 0/1:

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

Related Commands

Command	Description
-	-

Platform Description

N/A

show version

To view the information of the system, execute the command show version in the privileged EXEC mode.

show version [**devices** | **module** | **slots**]

Parameter Description

Parameter	Description
devices	Current device information
module	Current module information of the device.
slots	Current slot information of the device.

Defaults

-

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to view current system information, mainly including the system start time, version information, device information, serial number ,etc.

Configuration Examples

The example below shows the system information.

```
Ruijie# show clock detail
clock: 2003-3-17 10:27:21
Clock read from calendar when system boot.
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
-	-

Platform Description

N/A

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
-	-

Defaults -

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The example below is an execution 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
-	-

Platform Description -

speed

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

speed *speed*

Parameter Description

Parameter	Description
speed	Transmission rate (bps) on the terminal. For serial ports, the optional rates are 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 sets the speed at which the terminal transmits packets.

Configuration Examples

The following example shows how to configure the rate of the serial port to 57600 bps:

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

Related Commands

Command	Description
-	-

Platform Description

-

telnet

To log in one server which supports the telnet connection, use the **telnet** command to log on in the 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 host or host name to be logged in.
port	Select the TCP port number to be used for the login, 23 by default.
/**source**	Specify the source IP or source interface used by the Telnet client.
ip *A.B.C.D*	Specify the source IPv4 address used by the Telnet client.
ipv6 *X:X:X:X::X*	Specify the source IPv6 address used by the Telnet client.
interface *interface-name*	Specify the source interface used by the Telnet client.
/**vrf** *vrf-name*	Specify the VRF routing table to be queried.

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

This command is used to log in a telnet server.

Configuration Examples

Example 1 commands telnet to 192.168.1.11, the port uses the default value, and the source interface is specified as Gi 0/1, the queried VRF route table is specified as vpn1.

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

Example 2 commands telnet to 2AAA:BBBB::CCCC

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

Related Commands

Command	Description
ip telnet source-interface	Specify the IP address of the interface as the source address for the Telnet connection.
show sessions	Show the currently established Telnet sessions.
exit	Exit current connection.

Platform Description

N/A

username

To set the local username, execute the global configuration mode command username.

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
encrypted-password	Password text
privilege-level	User bound privilege level

Defaults

-

Command Mode

Global configuration mode.

Usage Guide

This command is used to establish local user database for the purpose of authentication.

Caution

If the type of encryption is specified as 7, the length of the entered legal cipher text should be even.

Caution

In general, it is not necessary to specify the type of encryption as 7. Commonly, it is necessary to specify the type of encryption as 7 only when the encrypted password is copied and pasted.

Configuration Examples

The example below 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	Enable local authentication

Platform Description

-

username permission

Use the **username permission** command in the global configuration mode to configure operation permissions of specified files for local users.

username *name* **permission** *oper-mode filename*

no username *name* **permission** *oper-mode filename*

Parameter Description

Parameter	Description
name	It specifies the user name.
oper-mode	It specifies the operation permission.
filename	It specifies the file name or catalogue name.

Defaults

-

Command Mode

Global configuration mode

Usage Guide

This command is used to specify permissions to specified files for users.

Configuration Examples

Example 1 allows the user test to read and write all files and catalogs:

```
Ruijie(config)# username test permission rw /
```

Example 2 forbids the user test to process all files and catalogs:

```
Ruijie(config)# username test permission null /
```

Example 3 configures the user test to have permissions to read, write and execute all files and catalogs except for the file config.text.

```
Ruijie(config)# username test permission 0 /config.text
Ruijie(config)# username test permission rwx /
```

Related Commands

Command	Description
-	-

Platform Description

-

write

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

write [memory | network | terminal]

Parameter Description

Parameter	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 N/A

Command Mode Privileged EXEC mode

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

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.

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]
```

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

HTTP Service Configuration Commands

enable service web-server

Use this command to enable the HTTP service function. Use the **no** form of the 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 HTTP service.
https	Enables HTTPS service.
all	Enables both HTTP and HTTPS service.

Defaults

HTTP service function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If the command is followed by no key work or is followed by **all**, the HTTP and HTTPS services are both enabled; if the command is followed by **http**, only HTTP service is enabled; if the command is followed by **https**, only HTTPS service is enabled.

Use **no enable service web-server** to disable the HTTP service.

Configuration Examples

The following example enables both HTTP and HTTPS service functions.

```
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	Shows the system's current service status.
show web-server status	Shows the web server status.

Platform Description

-

http check-version

Check information about files that can be upgraded in the HTTP server.

http check-version

Parameter

Parameter	Description

Description

-	-

Defaults

-

Command Mode

Privileged mode

Usage Guide

You can use this command to check files that should be upgraded. Files detected on the server are the latest.

Configuration Examples

The following example checks HTTP upgrade version.

```
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	Upgrades specific files manually.

Platform Description

N/A

http update

Use this command to upgrade files manually.

http update web [**version** *string*]

Parameter Description

Parameter	Description
string	Version information about the upgrade Web package

Defaults

-

Command Mode

Privileged mode

Usage Guide

You can use this command to instruct the device to download the upgrade Web package from the remote server.

If the **version** information is specified, the device will be upgraded to the specified version; otherwise, the latest Web package will be used for upgrade.

Configuration Examples

The following example downloads the latest Web package manually from the remote server.

```
Ruijie#http update web
```

Related Commands

Command	Description
http check-vesion	Detects information about files that can be upgraded in the HTTP server.

Platform Description

N/A

http update mode

Use this command to configure HTTP upgrade mode.

http update mode auto-detect

no http update mode

Parameter Description

Parameter	Description
auto-detect	Auto detect mode

Defaults

The auto detect function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

You can use this command to configure the HTTP upgrade mode.

If this command is configured, in the auto detect mode, the device will detect files on the server during upgrade. Users can view which Web version is available for upgrade in the Web interface.

If you use the no form of the command, the manual upgrade mode is enabled and the device will not upgrade automatically unless you manually upgrade the device.

Configuration Examples

The following example changes the upgrade mode to 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
-	-

Platform Description

N/A

http update server

Use this command to configure the server address and port number for HTTP upgrade.

http update server { *host-name* | *ip-address* } [**port** *port-number*]

no http update server

Parameter Description

Parameter	Description
host-name	Server's domain name
ip-address	Server's address
port-number	Server's port number, which ranges from 1 to 65535

Defaults

The default server address is 0.0.0.0 and port number is 80.

Command Mode

Global configuration mode

Usage Guide

You can use this command to configure the server address and port number for HTTP upgrade. During HTTP upgrade, the device will first seek to connect to the server address configured by this command. If it fails to connect to the address, it will seek to connect to addresses in the local record. If no address can be connected, the upgrade fails.

The system will record one or multiple addresses of upgrade server. These addresses cannot be modified.

⚠ Caution

Users do not need to configure the server address as the local upgrade record file has recorded possible upgrade server addresses.

To configure the server domain name, users need to enable the device’s DNS function and configure the DNS server address.

Server address does not support IPV6.

Configuration Examples

The following example configures the server address and port number for HTTP upgrade.

```
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
-	-

Platform Description

N/A

http update time

Use this command to configure the HTTP upgrade auto detect time.

http update time daily *hh*:*mm*

no http update time

Parameter Description

Parameter	Description
hh:*mm*	Specific upgrade time; the format is: hour (based on 24 hour system):minute

Defaults

he default upgrade time is random.

Command Mode

Global configuration mode

Usage Guide

You can use this command to configure the HTTP auto detect time. The device will connect to Web server (rgos.ruijie.com.cn) on the configured time everyday to detect files that can be upgraded. Information of files acquired can be viewed on the Web interface.

If the no form of the command is used, the detect time is random.

Configuration Examples

The following example configures the HTTP auto upgrade 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 HTTP upgrade mode.

Platform Description

N/A

http web-file update

Use this command to upgrade Web package.

http web-file update

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged mode

Usage Guide

When the latest Web package is detected and downloaded to the device, you can run this command to update the Web package without restarting the device.

Caution You need to log in to the Web page again to make the new Web package effective.

Configuration Examples

The following example updates the Web package.

```
Ruijie#http web-file update
```

Related Commands

Command	Description
-	-

Platform Description

-

ip http authentication

Use this command to set the Web login verification mode. Use the **no** form of the command to restore the default configuration.

ip http authentication { **enable** | **local** }

no ip http authentication

Parameter Description

Parameter	Description
enable	Adopts the password set with the **enable password** or **enable secret** command for verification, the password must be 15 level.
local	Uses the local **username** and password set with the username command for verification. The user must be bond with the 15 authority level.

Defaults

The **enable** verification mode is adopted by default.

Command Mode

Global configuration mode

Usage Guide

When Http Server is used, you need to log in and pass the verification to enter the Web page. You can use this command to set the web login verification mode.

Configuration Examples

The following example sets the verification mode as local.

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip http authentication local
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.

Platform Description

N/A

ip http port

Use this command to set the HTTP service's port. Use the **no** form of the command to restore the default port.

ip http port *port-number*

no ip http port

Parameter Description

Parameter	Description
port-number	Sets the HTTP service port, which is 80 or ranges from 1025 to 65535.

Defaults The default port number is 80.

Command Mode Global configuration mode

Usage Guide You can use this command to set HTTP service's port.

Configuration Examples

The following example sets HTTP service's 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.
show web-server status	Shows the web server status.

Platform Description -

ip http secure-port

Use this command to set the HTTPS service's port. Use the **no** form of the command to restore the default port.

ip http secure-port ***port-number***

no ip http secure-port

Parameter Description

Parameter	Description
port-number	Sets the HTTPS service port, which is 443 or ranges from 1025 to 65535.

Defaults The default port number is 443.

Command Global configuration mode

Mode

Usage Guide

You can use this command to set HTTPS service's port.

Configuration Examples

The following example sets HTTPS service's 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.
show web-server status	Shows the web server status.

Platform Description

-

show web-server status

Use this command to show Web service configuration information and status.

show web-server status

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged mode

Usage Guide

-

Configuration Examples

The following example shows the Web service configuration information and status.

```
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.
ip http port	Sets HTTP service's port.
ip http secure-port	Sets HTTPS service's port.

Platform

-

Description

UPGRADE Configuration Commands

upgrade system

To upgrade the system, run the **upgrade system** command in privileged EXEC mode.

upgrade system [*filename*]

Parameter Description

Parameter	Description
filename	Name of the system upgrade file. This is an optional parameter. If the parameter is not specified, the upgrade uses the main program installation package of the current device.

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

Run this command to upgrade the system.

Note

Before running this command, download the software of the required version to the device. In addition, reset the device after usage, so that the device can run on the new version.

You cannot run the **upgrade system** command to degrade the system to a version earlier than 10.4(2). If the version of the manually installed software is earlier than 10.4(2), the following fault occurs in the system:

```
File [chars] is not an install package(version 2.0).
```

Specifically, [**chars**] indicates the name of the current main program file in the system.

Configuration Examples

Example: Run the **upgrade system** command to upgrade the system.

```
Ruijie#upgrade system rgos.bin
These images in linecard will be updated:
   Slot   image   linecard
   ----   -----   ----------------
      1   MAIN    M8600-24GT/12SFP
      6   MAIN    M8600-24SFP/12GT
-------------------------------------
(Slot 1): Installing MAIN
(Slot 1): Download image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!![OK - 8,003,872 bytes]
Waiting for image installed....Complete
```

```
(Slot 1): MAIN installed.
(Slot 1): All images have been installed.
(Slot 6): Installing MAIN
(Slot 6): Download image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!![OK - 8,003,872 bytes]
Waiting for image installed....Complete
(Slot 6): MAIN installed.
(Slot 6): All images have been installed.
```

Related Commands

Command	**Description**
-	-

Platform Description

N/A

synchronize

To synchronize a certain file from the master device to each non-master device, run the **synchronize** command in the privileged EXEC mode.

synchronize *filename*

Parameter Description

Parameter	**Description**
filename	Name of the file to be synchronized. The file is located on the master device and supports only a **flash:** prefix.

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

Run this command to synchronize a specified file from the master device to each non-master device.

Note

The file synchronized to a non-master device is a file with the same name in the same path as the specified file on the master device.

Configuration Examples

Example: Run the **synchronize** *filename* command to synchronize the rgos.bin file from the master device to each non-master device.

```
Ruijie#synchronize flash:rgos.bin
Synchornize file /rgos.bin to slave:/
Device(6):                                                    download
```

```
file!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!![OK - 10,414,752 bytes]
Synchornize file to slave devices successfully!
```

Related Commands

Command	Description
-	-

Platform Description

N/A

LINE Configuration Commands

access-class

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

By default, no ACL is configured under Line. 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. By default, all the incoming and outgoing connections are allowed, and no connection is filtered. After **access-class** is configured, only the connections that pass access list filtering can be established successfully. Use the **show running** command to view configuration information under Line.

Configuration Examples

In 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

Platform Description

N/A

line

To enter the specified LINE mode, use the following command:

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

Parameter Description

Parameter	Description
aux	Auxiliary port, on the routers.
console	Console port
tty	Asynchronous port, on the routers.
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 can be used to increase the number of VTY connections currently available. The number of currently available VTY connections can be decreased by using the **no** form of this command.

line vty *line-number*

no line vty *line-number*

Parameter Description

Parameter	Description
line-number	The number of VTY connections.

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

Command Mode

Global configuration mode.

Usage Guide

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

Configuration Examples

Increase the number of available VTY connections to 20. The available VTY connections are numbered 0 to 19.

```
Ruijie(config)# line vty 19
Decrease the number of available VTY connections to 10. The available VTY
connections are numbered 0-9.
Ruijie(config)# line vty 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

transport input

To set the specified protocol under Line that can be used for communication, use the **transport input** command. Use the **default transport input** command 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 of protocols under Line to be used for communication

Defaults

By default, VTY allows all the protocols to be used for communication. The default value of other types of TTYs is NONE, indicating that no protocols are allowed for communication. After some protocols are set to be 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 that are 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

Specify 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

Platform Description

N/A

File System Configuration Commands

cd

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

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

Parameter Description

Parameter	Description
filesystem:	Specified file system. This parameter must be carried with ":".
directory	Specified directory

Defaults The default directory is the flash root directory.

Command Mode Privileged EXEC mode.

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

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

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

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

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

Related Commands

Command	Description
pwd	Show the present word 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.

destination-url	Destination file URL, which can be local or remote.

Defaults N/A

Command Mode Privileged EXEC mode.

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

The following table lists the URL prefix for the specified file system:

Prefix	Description
flash:	Flash storage media. This prefix can be used in all devices. The default is flash if the prefix is not used for the URL. In general, the bootstrap main program is stored in the flash.
tftp:	TFTP network server
xmodem:	Use the xmodem protocol to transmit the file to the network device.
slave:	Flash on the slave 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 M1 slot of the chassis with switch id 2, in the VSU mode.

Note

1. This command does not support the wildcard.

2. Without the specified URL prefix configured, it refers to the current file system.

3. When specify the URL prefix, make sure the path goes after the colon ":" is an absolute path. But there is an exception: the local flash file system (with flash prefix keywords) still supports relative paths, but only when the current catalog is in the local flash.

4. Different file system commands and different product platforms support different types of file systems, and the operating prefix combination supporting conditions of file system are also different. The use of the command depends on the real situations. For the details of the supported file system services of the current commands, refer to the help information in the command lines.

Configuration Examples Example 1: Download the file from the tftp server:

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

Example 2: Upload the file to the tftp server:

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

Example 3: Use the xmodem protocol to download the file:

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

Example 4: Copy the file to the U disk:

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

Example 5: Copy the file to the slave management board:

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

Example 6: Copy the file from the flash to the SD card:

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

Example 7: Copy the file from the U disk to the SD card:

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

Example 8: Copy the file from the SD card to the U disk:

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

Example 9: Obtain the command line help to judge which file system prefix combinations are supported by the current products and versions.

```
Ruijie#copy ?
  WORD            Copy from current file system
  flash:          Copy from flash file system
  ftp:            Copy from ftp: file system
  help            Help informatioin
  running-config  Copy from current system configuration
  startup-config  Copy from startup configuration
  tftp:           Copy from tftp: file system
  usb0:           Copy from usb0 file system
  usb1:           Copy from usb1 file system
  xmodem:         Copy from xmodem: file system

Ruijie#copy tftp://172.18.2.18/rgos.bin ?
  WORD            Copy to current file system
  flash:          Copy to flash: file system
  running-config  Update (merge with) current system configuration
  startup-config  Copy to startup configuration
  usb0:           Copy to usb0 file system
  usb1:           Copy to usb1 file system
```

Related

Command	Description

Commands

delete	Delete the file.
rename	Rename the file.
dir	Show the file list of the specified directory.

Platform Description

N/A

delete

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

delete url

Parameter Description

Parameter	Description
url	The URL for 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 supports deleting the files stores in the local storage media, i.e., the URL must be one of the flash:/ usb0:/ or usb1:/ slave:/. If the prefix is not specified in the URL, it indicates to delete the file in the system.

Note This command does not support the wildcard.

Configuration Examples

Example 1: Delete the `tmpfile` from the present directory:

```
Ruijie# delete tmpfile
```

Example 2: Delete the `rgos.bin.bak` from the secondary board:

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

Example 3: Delete the `aaa.bin` form the SD card:

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

Related Commands

Command	Description
copy	Copy the file.
dir	Show the file list of the specified directory.

Platform

N/A

Description

dir

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

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

Parameter Description

Parameter	Description
filesystem	Set the file system for the file to be displayed. This parameter must carry with ”:”.
directory	Set the directory for the file to be displayed.

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

Command Mode Privileged EXEC mode.

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

Note This command does not support the wildcard.

Configuration Examples Example 1: Show the file information of the root directory in the slave 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: Show the information of all the 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	Show the present directory.
cd	Set 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.

Usage Guide

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

Note

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

Configuration Examples

Example 1: Create the test directory at the root directory:

```
Ruijie# mkdir test
```

Example 2: Create the test2 directory at the root directory of the SD card:

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

Related Commands

Command	Description
rmdir	Delete the directory.

pwd	Show 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	The source file URL to move.
url2	The URL of the destination file or directory.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide This command only supports to move the local file, but not to transfer the file to the server using the protocol. The supported prefixes are: usb0/1, flash and slave.

Configuration Examples Example 1: Move the log.txt to the upper-level directory and rename it config.txt:

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

Example 2: Move the log.txt in the slave board to the usb0 device:

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

Example 3: Rename the log.txt in the present directory as log.txt.bak:

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

Example 4: Move the rgos.bin in the SD card to the flash:

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

Example 5: Move the test.txt in the U disk to the SD card:

```
Ruijie#  rename  usb0:/test.txt  sd0:/test2.txt  config-interface-vfc)#bind
mac-address 001d.0928.b62f
```

Related Commands

Command	Description
delete	Delete the file.
copy	Copy the file.

Platform N/A

Description

rmdir

Use this command to delete an empty 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 the wildcards, and the directory to be deleted must be empty. Since this command supports abbreviations, you can also use the **rm** command to delete empty directories.

Configuration Examples If there is tmp directory in the present directory and the directory does not contain any files:

```
Ruijie# rmdir tmp
Ruijie# ls
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

pwd

Use this command to show the working path.

pwd

Parameter Description

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

Defaults N/A

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	Change the file system in the present directory.

Platform Description N/A

show file systems

Use this command to show the file system information.

show file systems

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

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

Configuration Examples Show the file system information:

```
Ruijie# show file systems
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

Configuration Commands of Configuration File Management

archive

Use this command to switch to the archive configuration mode. The **no** form of this command can be used to restore all configurations in the archive configuration mode to the default state.

archive

no archive

Parameter description

Parameter	Description
-	-

Default

-

Command mode

Global configuration mode.

Usage guidelines

Use the **archive** command to switch to the archive configuration mode.

Use the **end** command or enter CTRL+C to return to the privileged EXEC mode.

Use the **exit** command to return to the global configuration mode.

Examples

The following example switches to the archive configuration mode:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
```

Related commands

Command	Description
-	-

hidekeys

Use this command to prohibit showing the passwords in the configuration log. The **no** form of this command can be used to allow showing the passwords in the configuration log.

hidekeys

no hidekeys

Parameter description

Parameter	Description
-	-

Default

Allow showing the passwords in the configuration log by default.

Command mode

Archive log management configuration mode

Usage guidelines

N/A.

Examples

The following example prohibits showing the passwords in the configuration log:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# hidekeys
```

Related commands

Command	Description
archive	Enter the archive configuration mode.
log config	Enter the archive log management configuration mode.
logging enable	Enable the function of logging the configuration change

log config

Use this command to switch to the archive log management configuation mode. The no form of this command is used to restore all configurations in this configuration mode to the default state.

log config

no log config

Parameter description

Parameter	Description
-	-

Default

N/A.

Command mode

Archive configuration mode

Usage guidelines

Use the **log config** command to switch to the archive log management configuration mode.

Use the **end** command or enter CTRL+C to return to the privileged EXEC mode.

Use the **exit** command to return to the archive configuration mode.

Examples

The following example switches to the archive log management configuration mode:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
```

Related commands

Command	Description
archive	Enter the archive configuration mode.

logging enable

Use this command to enable the function of logging the configuration change. The **no** form of this command is used to disable this function.

logging enable

no logging enable

Parameter description

Parameter	Description
-	-

Default

Disabled

Command mode

Archive log management configuration mode

Usage guidelines

N/A

Examples

The following example enables the function of logging the configuration change:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# logging enable
```

Related commands

Command	Description
archive	Enter the archive configuration mode.
log config	Enter the archive log management configuration mode.

logging size

Use this commad to specify the maximum number of the entries saved in the configuration log. The **no** form of this command is used to restore it to the default value.

logging size *entries*

no logging size

Parameter description

Parameter	Description
entries	The maximum number of the entries saved in the configuration log, in the range of 1 to 1000.

Default 100

Command mode Archive log management configuration mode

Usage guidelines N/A

Examples

The following example specifies the maximum number of the entries saved in the configuration log as 50:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# logging size 50
```

Related commands

Command	Description
archive	Enter the archive configuration mode.
log config	Enter the archive log management configuration mode.

notify syslog

Use this command to allow sending the configuration change notification to the remote log server. The **no** form of this command can be used to prohibit sending the configuration change notification to the remote log server.

notify syslog

no notify syslog

Parameter description

Parameter	Description
-	-

Default

Prohibit sending the configuration notification to the remote log server by default.

Command mode

Archive log management configuration mode

Usage guidelines

N/A

Examples

The following example allows sending the configuration change notification to the remote log server:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# archive
Ruijie(config-archive)# log config
Ruijie(config-archive-log-config)# notify syslog
```

Related commands

Command	Description
archive	Enter the archive configuration mode.

	log config	Enter the archive log management configuration mode.
	logging enable	Enable the function of logging the configuration change.

show archive log config

Use this command to show the entry information of the configuraiton log.

show archive log config {{**all** | *start-num* [*end-num*]} [**provisioning** | **contenttype** [**plaintext**]] | **statistics**}

Parameter description

Parameter	Description
all	Show all entry information of the configuration log.
start-num [*end-num*]	Specifying the *start-num* means showing all configuration logs starting with this record. If the end-num is specified at the same time, it will show the configuration logs with the record number between the *start-num* and *end-num*. if the *start-num* is 0, it will show the configuration logs from the first entry. If the end-num is 0, it will show all configuration logs starting with the *start-num*. The *start-num* and *end-num* are both in the range of 0 to 2147483647.
provisioning	Show the configuration logs in the format shown in the configuration file.
contenttype	Specify the showing format of the configuration logs.
plaintext	Specify the configuration logs to be shown in the ordinary text format.
statistics	Show the memory usage of the configuration log.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

The *start-num* patameter must be specified when showing the configuration logs without the **all** specified. Use the *end-num* parameter to specify the range of the configuration logs to be viewed. When the configuration log entry that corresponding to the specified *end-num* is not existent, show all configuration logs from the *start-num* to the record number that is less than the *end-num*.(if the *end-num* is specified to 0, show all configuration logs starting with the *start-num*). On condition that the configuration log entry that corresponding to the specified *start-num* is not existent, show the configuration logs starting with the record number that is larger than the *start-num*. If the provisioning is specified, show the configuraitons in the format that is in the configuration files.

Examples

The following example shows the configuration logs numbered 1 to 2:

```
Ruijie# show archive log config 1 2
idx sess  user@line   datetime     logged command
1   1  unknown@console  Mar 21 09:57:22  | logging enable
2   1  unknown@console  Mar 21 09:57:46  | logging size 50
```

Field	Description
idx	The record number of the configuration log entry.
sess	Session number related to this configuration log entry.
user@line	Username and line name of generating this configuration log entry.
datetime	Time of generating this configuration log entry.
logged command	Executed configuration command.

The following example shows all configuration logs in the format of configurations shown in the configuration file.

```
Ruijie# show archive log config all provisioning
archive
 log config
  logging enable
  logging size 50
```

The following example shows the memory usage of the configuration log.

```
Ruijie# show archive log config statistics
```

```
Config Log Session Info:
  Number of sessions being tracked: 1
  Memory being held: 1270 bytes
  Total memory allocated for session tracking: 1270 bytes
  Total memory freed from session tracking: 0 bytes
Config Log log-queue Info:
 Number of entries in the log-queue: 3
  Memory being held in the log-queue: 671 bytes
  Total memory allocated for log entries: 671 bytes
  Total memory freed from log entries:: 0 bytes
```

Related commands

Command	Description
-	-

CPU-LOG Configuration Commands

cpu-log

Use this command to manually configure the low and high threshold of triggering the cpu utilization log.

cpu-log log-limit *low_num high_num*

Parameter Description

Parameter	Description
log-limit	The command descriptor prompting the limit range.
low_num	Sets the low threshold of triggering the cpu utilization log.
high_num	Sets the high threshold of triggering the cpu utilization log.

Defaults By default, the high and low threshold of triggering the cpu utilization log are 100% and 90%.

Command Mode Global configuration mode.

Usage Guide Use this command to manually configure the low and high threshold of triggering the cpu utilization log. When the CPU utilization exceeds the high threshold, the system prompts the log message for one time. When the CPU utilization is less than the low threshold, the system prompts the log message and advertises that the current CPU utilization has been decreased. This message is sent only when the CPU high and low threshold switches over.

Configuration Examples #Show how to set the low and high threshold of triggering the cpu utilization log to 70% and 80% respectively.

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

#The console prompts the following message when the CPU utilization is higher 80%:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute: 95%,
Using most cpu's task is ktimer : 94%
```

#The console prompts the following message when the CPU utilization is less than 70%:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU
utilization in one minute :68%,Using most cpu's task
is ktimer : 60%
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: The CPU
using rate has down!
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show cpu

Use this command to show the CPU utilization information.

show cpu

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to show the system CPU utilization information in five seconds, one minute and five minutes, and the CPU utilization of every task in five seconds, one minute and five minutes.

Configuration Examples

```
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 three lines indicate the system CPU utilization in five seconds, one minute and five minutes, including LISR, HISR and tasks. Then, it describes the detailed CPU utilization distribution:

- No: Serial number
- 5Sec: CPU utilization of the tasks in five seconds.
- 1Min: CPU utilization of the tasks in one minute.
- 5Min: CPU utilization of the tasks in five minutes.

The first two lines in the list above indicate the CPU utilization of all LISRs and HISRs. From the third line, it begins to indicate the CPU utilization of the tasks. The last line indicates the CPU utilization of the idle task, which is the same as the “System Idle Process” in the Windows. In the example above, CPU utilization of idle task within five seconds is 75%, indicating that 75% CPU is idle.

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

Memory Commands

show memory

Use this command to show the memory usage.

show memory

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

Use this command to show the system memory state and usage information, including the system physical memory, the number of free pages and free memory.

Configuration Examples

This example shows the running result of the command **show memory**.

```
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 the following parts:

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

Watermarks	Description
min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fails to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One routing 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	The memory resources are insufficient. The routing 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	The memory resources are sufficient. Each routing protocol attempts to restore the state from OVERFLOW to normal.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Syslog Configuration Commands

clear logging

Use this command to clear the logs from the buffer.

clear logging

Parameter Description

Parameter	Description
-	-

Defaults -

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	Record logs on different devices.
show logging	Show the logs in the buffer.
logging buffered	Record the logs to the memory buffer.

Platform Description -

logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs. The **no** form of this command disables recording logs in memory buffer. The **default** form of this command restores the memory buffer size to the default value.

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

no logging buffered

default logging buffered

Parameter

Parameter	Description

Description

buffer-size	Size of the buffer is related to the specific device: For the kernel / aggregation switches, 4K to 10M bytes. For the access switches, 4K to 1M Bytes. For other devices, 4K to 128K Bytes.
level	Severity of logs, 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.
kernel switches: 1M Bytes;
aggregation switches: 256K Bytes;
access switches: 128K Bytes;
other devices: 4K 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 it is full, the oldest information will be overwritten. To show the log information in the memory buffer, run the **show logging** command at the privileged user level.

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 by privileged user. To trace a problem, it is required to record logs in flash or send them to Syslog Server.

The log information of the RGOS is classified into the following 8 levels:

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 specified device, the log information is at or below the set level will not 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 configuration example below 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	Record logs on different devices.
show logging	Show the logs in the buffer.
clear logging	Clear the logs in the log buffer.

Platform Description

-

logging console

Use this command to set the severity of logs that are allowed to be displayed on the console. The **no** form of the command disables displaying the logs 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 here, 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 example below 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	Record logs on different devices.

show logging	Show the logs and related log configuration parameters in the buffer.

Platform Description

-

logging count

Use this command to enable the log statistics function. The **no** form of the command deletes the log statistics and disables the statistics function.

logging count

no logging count

Parameter Description

Parameter	Description
-	-

Defaults

Disabled.

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 **no logging count**, 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	Show the log statistics.
show logging	Show the logs and related log configuration parameters in the buffer.

Platform Description

-

logging facility

Use this command to configure the log device. The **no** form of the command restores it to the default device value (23).

logging facility *facility-type*

no logging facility

Parameter Description

Parameter	Description
facility-type	Syslog device value. For detailed configuration value, refer to the usage guidelines.

Defaults

Local7(23).

Command Mode

Global configuration mode.

Usage Guide

The following table (Table-2) is the possible device value of Syslog:

Table-2

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization message
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer system
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization message
11 (ftp)	FTP daemon
12 (ntp)	NTP daemon
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

Following is to set the device value of **Syslog** as **kernel**:

```
Ruijie(config)# logging facility kern
```

Related Commands

Command	Description
logging console	Set the severity of logs that are allowed to be displayed on the console.

Platform Description

-

logging file flash

Use this command to record logs in the flash. The **no** form of the command disables 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 128K to 6M bytes, 128K bytes by default
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, please see Table-1.

Defaults

Logs are not recorded in the FLASH.

Command Mode

Global configuration mode.

Usage Guide

If no **Syslog Server** is specified or it is not desired to transfer logs in the network due to the consideration of security purpose, it is possible to save the logs directly in flash.

The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.

To record the logs into the expansion FLASH, The expansion FLASH is required. If there is no expansion FLASH, the logging file flash will be hidden automatically and the related configuration will be denied.

Configuration Examples

The example below records the logs into the expansion FLASH, with the name trace.txt, file size 128K and log severity 6.

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

Related Commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.
more flash	View the logs in the flash.

Platform Description

-

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.). The **no** form of the command disables displaying the logs 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 messages on the VTY window, execute first the privileged user command **terminal monitor**. The level of logs to be displayed is defined with **logging monitor**.
The log level defined with "Logging monitor" is for all VTY windows.

Configuration Examples

The example below 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	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.

Platform Description

-

logging on

Use this command to record logs on different devices. The **no** form of this command disables the function.

logging on

no logging on

Parameter Description

Parameter	Description
-	-

Defaults Logs are allowed to be displayed on different devices.

Command Mode Global configuration mode.

Usage Guide RGOS can not only show the log information in the Console window and VTY window, but also record it in different equipments such as the memory buffer, the 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 in the equipment.

```
Ruijie(config)# no logging on
```

Related Commands

Command	Description
logging buffered	Record logs to an internal buffer.
logging server	Record logs to the Syslog server.
logging file flash:	Record logs on the FLASH.
logging console	Set the log level to be displayed on the console.
logging monitor	Set the log level to be displayed on the VTY window (such as telnet window).
logging trap	Set the log level to be sent to the Syslog server.

Platform Description -

logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in global configuration mode. The **no** form of this command disables the 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 processed in a second with the range from 1 to 10000.
all	Set rate limit to all the logs with severity level 0-7.
console	Set the amount of logs 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 this severity level is not controlled.
severity	Log severity level with the range from 0 to 7. The lower the level is, the higher the severity is.

Defaults Disabled.

Command Mode Global configuration mode.

Usage Guide Use this command to control the syslog output to prevent the massive log output.

Configuration Examples The example below sets the number of the logs (including debug) 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	Show the log statistics.
show logging	Show the logs and related log configuration parameters in the buffer.

Platform Description -

logging rd on

Configure this command on the host in global configuration mode to enable log redirection in VSU environment, so that log information can be redirected from the slave or backup device to the host. Use the **no** form of this command to disable the log redirection function.

logging rd on

no logging rd on

Parameter Description

Parameter	Description
-	-

Defaults By default, the log redirection is enabled.

Command Mode Global configuration mode

Usage Guide Log information on the slave or backup device can be not only displayed on the Console window of the salve or backup device, but also be redirected to the host for output, including to the Console window and VTY window on the host, or be recorded on the memory buffer, extended FLASH and Syslog Server on the host.

Configuration The following example enables log redirection on the device:

Examples

```
Ruijie(config)#logging rd on
```

Related Commands

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

Platform Description

-

logging rd rate-limit

Configure the command on the host in global configuration mode to enable the rate limit on log redirection function in VSU environment and limit log information allowed to be redirected from the slave or backup device to the host per second. Use the **no** form of this command to disable the log redirection rate restricting function.

logging rd rate-limit *number* [**except** [*severity*]]

no logging rd rate-limit

Parameter Description

Parameter	Description
number	Log information allowed to be redirected per second, which ranges from 1 to 10000.
Except	No rate limit is imposed on log information on and below this error level. The default error level is error (3), no rate limit is imposed on log information on and below the error level.
severity	The error level ranges from 0 to 7. The lower the level is, the higher the severity is.

Defaults

By default, 200 logs can be redirected each second at most.

Command Mode

Global configuration mode

Usage Guide

This command is used to control output of redirected log information. Use this command to prevent massive log information from being redirected from the slave or backup device to the host.

Configuration Examples

The following example sets the number of logs, including debug, allowed to be redirected from the slave device to the host per second to 10. The limit is not imposed on logs on the warning or higher error level:

```
Ruijie(config)#logging rd rate-limit 10 except warnings
```

Related Commands

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

	in the log buffer.

Platform Description

-

logging server

Use this command to record the logs in the specified Syslog sever. The **no** form of the command deletes the Syslog server with specified address from the Syslog server list.

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	Receive IP address of the log server.
vrf-name	Specify VRF (VPN device forwarding list) connecting to the log server.
ipv6-address	Specify IPV6 address of the log server.

Defaults

By default, it does not send the logs to any syslog server.

Command Mode

Global configuration mode.

Usage Guide

This command specifies a Syslog server to receive the logs of the device. The RGOS allows the configuration of up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

Configuration Examples

The example below specifies a syslog server at address 202.101.11.1:

```
Ruijie(config)# logging server 202.101.11.1
The example below specifies an ipv6 address as AAAA:BBBB:FFFF:
Ruijie(config)# logging server ipv6 AAAA:BBBB:FFFF
```

Related Commands

Command	Description
logging on	Record logs on different devices.
show logging	Show the logs and related log configuration parameters in the buffer.
logging trap	Set the level of logs to be sent to Syslog server.

Platform Description

logging source interface

Use this command to configure the source interface of logs. The **no** form of the command cancels the source interface setting for the specified log.

logging source interface *interface-type interface-number*

no logging source interface

Parameter Description

Parameter	Description
interface-type	The type of interface
interface-number	The number of interface

Defaults

N/A.

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 address. If no source interface of the device or no IP address of the source interface is configured, the source IP address of the log message is still that of the interface from which the message is sent.

Configuration Examples

The example below specifies loopback 0 as the source address of the syslog messages:

```
Ruijie(config)# logging source interface loopback 0
```

Related Commands

Command	Description
logging server	Record logs to the Syslog server.

Platform Description

logging source ip| ipv6

Use this command to configure the source IP address of logs. The **no** form of the command cancels the source IP address setting for the specified log.

logging source {**ip** *ip-address* **| ipv6** *ipv6-address*}

no logging source {**ip | ipv6**}

Parameter Description

Parameter	Description
ip-address	Specify the source IPV4 address sending the logs to IPV4 log server.

ipv6-address	Specify the source IPV6 address sending the logs to IPV6 log server.

Defaults N/A.

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 address. If no IP address is configured for the device, the source IP address of the log message is still that of the interface from which the message is sent.

Configuration Examples The example below specifies the 192.168.1.1 as the source address of the syslog messages:

```
Ruijie(config)# logging source ip 192.168.1.1
```

Related Commands

Command	Description
logging server	Record logs to the Syslog server.

Platform Description -

logging synchronous

Use this command to enable synchronization function of user input and log output in the line configuration mode to prevent the user from interrupting when keying in the characters. The **no** form of this command disables this function.

logging synchronous

no logging synchronous

Parameter Description

Parameter	Description
-	-

Defaults

Disabled.

Command Mode

Line configuration mode.

Usage Guide

This command enables synchronization function of 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	View the configuration.

Platform Description

-

logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server. The **no** form of the command disables sending the logs 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 60-1.

Defaults

Informational(6).

Command Mode

Global configuration mode.

Usage Guide

To send logs to the Syslog Server, execute first the global configuration command **logging** to configure the **Syslog Server**. Then, execute **logging trap** to specify the severity of logs to be sent. The **show logging** command displays the related setting parameters and statistics of the log.

Configuration Examples

The example below enables logs at severity 6 to be sent to the Syslog Server at address 202.101.11.22:

```
Ruijie(config)# logging 202.101.11.22
Ruijie(config)# logging trap informational
```

Related Commands

Command	Description
logging on	Reocrd logs on different devicds.
logging	Record logs to the Syslog server.
show logging	Show the logs and related log configuration parameters in the buffer.

Platform Description

-

more flash

Use this command to show the contents of the logs stored in the FLASH.

more flash:*filename*

Parameter

Parameter	Description

Description

filename	Log file name

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

In the FLASH, the log file means 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 FLASH as you can see:

```
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	Record the logs to the FLASH.

Platform Description

-

service private-syslog

Use this command in global configuration mode to adjust the log format to the private log display format. Use the **no** form of this command to remove the configuration and restore the default log format.

service private-syslog

no service private-syslog

Parameter Description

Parameter	Description
-	-

Defaults

Log information is displayed in the default log format.

Command Mode

Global configuration mode

Usage Guide

By default, the log information on the device is displayed in the following format:
*timestamp: %facility-severity-mnemonic: description
*timestamp: %module name-severity level-information about mnemonic: detailed log information
For example: *May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console

If the private log formation format is enabled, the log information on the device is displayed as follows:

timestamp facility-severity-mnemonic: description

timestamp module name-severity level-information about mnemonic: detailed log information

For example: May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console

The differences between the private and the default log format lie in timestamp and identification string. In the private log format, there is no "*" before the timestamp and no ":" after it and no "%" before the identification string.

Configuration Examples

The following example adjusts the log format to the private one:

```
Ruijie(config)# service private-syslog
```

Related Commands

Command	Description
logging on	Turn on the log switch.
service timestamps	Enable the timestamp in log information.

Platform Description

-

service sequence-numbers

Use this command to attach sequential numbers into the logs. The **no** form of the command removes the sequential numbers in the logs.

service sequence-numbers

no service sequence-numbers

Parameter Description

Parameter	Description
-	-

Defaults

No sequential numbers are attached.

Command Mode

Global configuration mode.

Usage Guide

In addition to the timestamp, it is possible to add sequential 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 example below adds sequential numbers to the logs.

```
Ruijie(config)#  service sequence-numbers
```

Related Commands

Command	Description
logging on	Record logs on different devices.
service timestamps	Attach the timestamp to the logs

Platform Description

-

service standard-syslog

Use this command in global configuration mode to adjust the log format to the one defined in standard RFC3164. Use the **no** form of this command to remove the configuration and use the default log format.

service standard-syslog

no service standard-syslog

Parameter Description

Parameter	Description
-	-

Defaults

Log information is displayed in the default log format.

Command Mode

Global configuration mode

By default, the log information on the device is displayed in the following format:
*timestamp: %facility-severity-mnemonic: description
*timestamp: %module name-severity level-information about mnemonic: detailed log information
For example: *May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console

Usage Guide

If the standard log format is enabled, the log information on the device is displayed as follows:
timestamp %facility-severity-mnemonic: description
timestamp %module name-severity level-information about mnemonic: detailed log information
For example: May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console
The difference between the standard and default log format lies in the timestamp. In the standard log format, there is no “*” before the timestamp and no “:” after it.

Configuration Examples

The following example adjusts the log format to the standard one:

```
Ruijie(config)# service standard-syslog
```

Related Commands

Command	Description
logging on	Turn on the log switch.
service timestamps	Enable the timestamp in log information.

Platform Description

-

service sysname

Use this command to attach system name to logs. The **no** form of this command removes the system name from the logs.

service sysname

no service sysname

Parameter Description

Parameter	Description
-	-

Defaults

No system name is attached.

Command Mode

Global configuration mode.

Usage Guide

This command allows you to decide whether to add system name in the log information.

Configuration Examples

Add 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	Show the logs and related log configuration parameters in the buffer.

Platform Description

-

service timestamps

Use this command to attach timestamp into logs. The **no** form of this command removes the timestamp from the logs. The **default** form of this command restores the timestamp configuration to the defalt.

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 types of log, including **Log** and **Debug**. The **log** type means the log information with severity levels of 0 to 6. The **debug** type means 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 example below 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	Record logs on different devices.
service sequence-numbers	Attach sequential number to logs.

Platform Description

-

show logging

Use this command to show parameters and statistics information about logs and the logs in the buffer.

show logging

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

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  %LINEPROTO-5-UPDOWN:  Line  protocol  on
Interface FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24,
changed state to up.
015492:  *Sep  19  02:46:28:  Ruijie  %LINEPROTO-5-UPDOWN:  Line  protocol  on
Interface FastEthernet 0/24, changed state to up.
```

The log messages are described as below:

Field	Description
Syslog logging	Logging switch: 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 log messages	Sequence switch
Sysname log messages	System name added to the log messages
Count log messages	Log statistical 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	Record logs on different devices.
clear logging	Clear the logs in the buffer.

Platform Description

-

show logging count

Use this command to show the log statistics.

show logging count

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

To use the log packet statistics function, run the **logging count** command in global configuration mode. The **show logging count** command can show the information of a log, occurrence times, and the last occurrence time.

You can use **show logging** command to check whether the log statistics function is enabled.

Configuration Examples

The following is the execution result of **show logging count**:

```
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	Enable the log statistics function.
show logging	Show the logs and related log configuration parameters in the buffer.
clear logging	Clear the logs in the buffer.

Platform Description

-

terminal monitor

Use this command to allow displaying log information on the current VTY window. Use the **no** form of this command to disable displaying log information on the current VTY window.

terminal monitor

terminal no monitor

Parameter Description

Parameter	Description
-	-

Defaults

By default, it is not allowed to display log information on the VTY window.

Command Mode

Privileged user mode

Usage Guide

This command is used to set temporary attributes of the current VTY. As a temporary attribute setting, it will not be saved permanently. After VTY terminal session finishes, the system will restore the default setting and this temporary attribute setting will lose effect. This command can be also used on the console, but it does not take effect.

Configuration Examples

The following example configures to allow printing log information on the current VTY window:

```
Ruijie# terminal monitor
```

Related Commands

Command	Description
-	-

Platform Description

-

Cluster Management Configuration Commands

cluster

Enter the cluster configuration mode. Use the **no** form of this command to delete a cluster.

cluster [*name*]

no cluster [*name*]

Parameter Description

Parameter	Description
name	Character string of a cluster name, containing a maximum of 31 characters. If the value is not specified, the default cluster name CLUSTER is used.

Defaults

No cluster is created.

Command Mode

Global configuration mode

Usage Guide

Use the **cluster** *name* command to create a cluster and enter the cluster configuration mode. The default SN is 1 for the cluster management device. The host number of the IP address is consistent with the SN.

After the command is configured, the cluster can run properly if the following conditions are met:

1) The device belongs to no cluster.

2) The Link Layer Discovery Protocol (LLDP) is running properly.

Use the **no** form of the command to delete the current cluster and all configurations in the cluster configuration mode.

Note

1. Use this command on a candidate device to create a cluster. If the cluster name is not specified, CLUSTER is used as the cluster name by default. The command cannot be used on a member device. Use the **cluster** command on the management device to enter the cluster configuration mode. Use the **cluster** *name* command to enter the cluster configuration mode if the name is the same as the name of the created cluster. If the name is different from the name of the created cluster, the cluster is considered as a new one, and you must delete the existing cluster and re-configure a new cluster.

2. In cluster creation, by default, the SN of the cluster management device is always 1 and the host number of the IP address is always consistent with the SN.

Configuration

Example 1: Use the following command to enter the cluster configuration mode:

Examples

```
Ruijie(config)#cluster
CLUSTER_1.Ruijie(config-cluster)#
```

Related Commands

Command	Description
cluster enable	Enable the cluster function for the device.
show cluster	Show basic information about the cluster that the device belongs to.
show cluster candidates	Show information about a candidate device.
show cluster member	Show information about a member device.
show cluster topology	Show topology information about the cluster.

Platform Description

N/A

cluster enable

Use this command to enable the cluster function on the device. Use the **no** form of this command to disable the cluster function.

cluster enable

no cluster enable

Parameter Description

Parameter	Description
-	-

Defaults

The cluster function is enabled on a device.

Command Mode

Global configuration mode

Usage Guide

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

⚠ Caution

If you use the **no** form of this command on the management device to disable the cluster function, the information of the cluster and the configurations will be deleted. If you use this command on a member device to disable the cluster function, the device is removed from the cluster and becomes a candidate device. If you use this command on a candidate device to disable the cluster function, the device cannot become a member of any cluster.

Configuration Examples

Example 1: Use the following command to disable the cluster function:

```
Ruijie(config)# no cluster enable
```

Related Commands

Command	Description
Cluster	Enter the cluster configuration mode.

Platform Description

N/A

cluster explore

Use this command on the management device to manually start topology collection.

cluster explore

Parameter Description

Parameter	Description
-	-

Defaults

None

Command Mode

Privileged EXEC mode

Usage Guide

Use this command on the management device to manually start topology collection. This command improves the cluster topology convergence.

⚠ Caution

This command can be used only on the management device.

Configuration Examples

Example 1: Use the following command to manually initiate the topology collection request:

```
CLUSTER_1.Ruijie#cluster explore
```

Related Commands

Command	Description
-	-

Platform Description

N/A

cluster login

Log in to the device. Use this command on the management device to log in to a member device for management, or use this command on a member device to log in to the management device. To return from the logged device, use the **exit** command in privileged EXEC mode.

cluster login { **administrator** | **member** { *member-id* | *H.H.H* }}

Parameter Description

Parameter	Description
member-id	The serial number of the member device to be logged in to.
H.H.H	The MAC address of the member device to be logged in to.

Defaults None

Command Mode Privileged EXEC mode

Usage Guide Use the **cluster login administrator** command to log in to the management device from a member device.

Use the **cluster login member** command to log in to a member device from the management device. To return from the logged device, use the **exit** command in privileged EXEC mode.

Caution

This command can be used only on the management and member devices.

Note

By default, you enter the user mode after logging in to the management device from a member device. To enter privileged EXEC mode, enter the password and pass the authentication.

During logging in, the console fails to respond if the cluster management IP address of the peer end is deleted or is changed to the **down** state. After timing out (three times the time specified in **timer hello** *hello-seconds,* and 90 seconds by default), the console returns to the original device. This occurs due to TCP features. In this case, the device needs to find another reachable path. Disconnection occurs if reconnection fails after timing out.

Configuration Examples Example 1: Use the following command to log in to member device 2 from the management device:

```
CLUSTER_1.Ruijie#cluster login member 2
```

Related Commands

Command	Description
show cluster	Show basic information about the cluster that the device belongs to.
show cluster member	Show information about a member device.
show cluster topology	Show topology information about the cluster.

Platform Description

N/A

cluster member

Specify the name or the MAC address of the cluster that manages the device. Use the **no** form of the command to delete the name or the MAC address of the cluster that manages the device.

cluster member { **cluster-name** *name* | **admin-address** *H.H.H* }

no cluster member

Parameter Description

Parameter	Description
name	Specify the name or MAC address of the cluster that manages the device.
H.H.H	Specify the MAC address of the cluster that manages the device.

Defaults

By default, the name or the MAC address of the cluster that manages the device is not specified.

Command Mode

Global configuration mode

Usage Guide

After this command is used, the device can be managed only by a specified cluster. After the **no** form of this command is used, the device can be managed by any cluster.

⚠ Caution

If this command is used on a member device and the specified cluster is different from the joined cluster, the member device initiatively exits the original cluster and joins the newly specified cluster. If the **no** form of this command is used, the specified cluster name or MAC address is deleted, but the member device does not exit the cluster.

After this command is run, the device only processes and forwards the specified cluster packets, and other cluster packets are discarded.

This command can be used only on the member and candidate devices.

Configuration Examples

Example 1: Use the following command to specify that the device can only join the cluster named Ruijie:

```
Ruijie(config)# cluster member cluster-name ruijie
```

Related Commands

Command	Description
-	-

Platform Description

N/A

cluster reload

In privileged EXEC mode, use this command on the management device to make a member device restart.

cluster reload member { *member-id* | *H.H.H* }

Parameter Description

Parameter	Description
member-id	ID of the member device to be restarted.
H.H.H	MAC address of the member device to be restarted.

Defaults

None

Command Mode

Privileged EXEC mode

Usage Guide

This command can be used to make a member device to restart.

Caution

This command can be used only on the management device.

Configuration Examples

Example 1: Use the following command to make member device 2 restart:

```
CLUSTER_1.Ruijie# cluster reload member 2
```

Related Commands

Command	Description
show cluster	Show basic information about the cluster that the device belongs to.
show cluster member	Show information about a member device.
show cluster topology	Show topology information about the cluster.

Platform Description

N/A

cluster tftp

In privileged EXEC mode, use this command to enable a member device to upload or download files, using the agent Trivial File Transfer Protocol (TFTP) of the cluster management device.

cluster tftp server: *source-file* **flash:** [*destination-file*]

cluster tftp flash: *source-file* **server:** [*destination-file*]

Parameter Description

Parameter	Description
source-file	The file to be transferred. The source file can be located on a local FLASH or remote TFTP server.
destination-file	The file to be transferred to. The destination file can be located on a local FLASH or remote TFTP server. If the destination file is not specified, the source file name is used the destination file name.

Defaults

None

Command Mode

Privileged EXEC mode

Usage Guide

Use the **cluster tftp server:** command to download files from the TFTP server to a local host.

Use the **cluster tftp flash:** command to upload files from a local host to the TFTP server.

Caution

Before using this command, ensure that you have used the **proxy tftp-server** command on the management device to set the cluster-sharing TFTP server.

This command can be used only on the management and member devices.

Configuration Examples

Example 1: Set the TFTP server 172.10.1.1 as the one shared by clusters. Then, access member device 2, and use the shared TFTP server to transfer the **config.text** file to a local host.

```
CLUSTER_1.Ruijie#configure terminal              //Run the command on the
command line interface (CLI) of the management device.
Enter configuration commands, one per line.  End with CNTL/Z.
CLUSTER_1.Ruijie(config)#cluster
CLUSTER_1.Ruijie(config-cluster)#proxy tftp-server 172.10.1.1
CLUSTER_1.Ruijie#cluster login member 2
CLUSTER_2.Ruijie#cluster tftp server://config.text flash:   //Run the cluster
TFTP agent.
```

Related Commands

Command	Description
proxy tftp-server	Set the cluster-sharing TFTP server.
show cluster	Show basic information about the cluster that the device belongs to.
show cluster candidates	Show information about a candidate device.
show cluster member	Show information about a member device.

Platform Description

N/A

hops-limit

Set the allowed hop count for topology collection from the farthest device to the cluster management device. Use the **no** form of this command to restore the default value.

hops-limit *hop-number*

no hops-limit [*hop-number*]

Parameter Description

Parameter	Description
hop-number	Hop count range for the cluster to discover devices. The range is 1–16 and the default value is 5.

Defaults

The default value is 5.

Command Mode

Cluster configuration mode

Usage Guide

Use this command to set the allowed hop count for topology collection from the farthest device to the cluster management device. That is the topology collection range, within which the cluster can discover devices.

Caution

When the topology collection range narrows down, the cluster management device removes the cluster devices beyond the new range from the topology table.

Configuration Examples

Example 1: Use the following command to set the allowed hop count to 4 for topology collection from the farthest device to the cluster management device:

```
CLUSTER_1.Ruijie(config-cluster)#hops-limit 4
```

Related Commands

Command	Description
show cluster	Show basic information about the cluster that the device belongs to.
show cluster candidates	Show information about a candidate device.
show cluster member	Show information about a member device.
show cluster topology	Show topology information about the cluster.

Platform Description

N/A

management

When a cluster is created, by default, the device configures the cluster management resources including the management Virtual LAN (VLAN) and IP address pool. Use the **no** form of this command to restore the default value.

management { **vlan** *vlan-id* **| ip-pool** *ip-address ip-mask* **| vlan** *vlan-id* **ip-pool** *ip-address ip-mask* }

no management [**vlan | ip-pool**]

Parameter Description

Parameter	Description
vlan-id	Cluster management VLAN ID. The range is 1 to4094.
ip-address	Cluster management IP address
ip-mask	Subnet mask of the cluster management IP address pool

Defaults

None

Command Mode

Cluster configuration mode

Usage Guide

Use the **management vlan** command to set the cluster management VLAN ID.

Use the **management ip-pool** command to set the cluster management IP address pool.

Use the **management vlan** *vlan-id* **ip-pool** *ip-address ip-mask* command to simultaneously set the cluster management VLAN ID and IP address pool.

By default, when you use the **no** form of this command:

The **no management** command is used to obtain the idle management resources within a specified range.

The **no management vlan** command is used to obtain the idle management VLAN ID within a specified range.

The **no management ip-pool** command is used to obtain the idle management IP address pool within a specified range.

Note

By default, the cluster automatically obtains the idle management VLAN within VLAN

2049 to 3000, and the idle management IP address pool within 192.168.168.0/24 to 192.168.254.0/24.

The cluster assigns matching *member-id* and *ip* to the management device and member device. Assume that the cluster management IP address is 192.168.176.0 255.255.255.0, and the subnet mask contains 24 digits. In this case: The allocable IP address count exceeds 240; The cluster assigns 1 as the management device SN and 192.168.176.1 as the IP address; The member device SN range is 2 to 240; The matching IP address range is 192.168.176.2 to 192.168.176.240. However, when the subnet mask contains less than 24 digits, for example 192.168.176.128 255.255.255.128: The IP address of the management device is 192.168.176.129; The IP host numbers 2 to 126 can be assigned to member devices (excluding IP host numbers consists of only zeros or all ones, and the one assigned to the management device); The member device SN range is 2 to 126.

In cluster creation, assume that: The obtained idle management IP address pool is 192.168.168.0 255.255.255.0; The maximum SN is 240; The device SN is 220. In this case, failure occurs if you use this command to set the management IP address pool to 192.168.176.0 255.255.255.128 because: The allocable IP address count is 126, including the IP address of the management device; However, the allocated SN 220 is greater than 126.

The VLAN ID and IP address are management resources and channels used in managing member devices inside the cluster. Therefore, cluster creation also fails when failure occurs in obtaining idle management resources.

Configuration Examples

Example 1: Use the following command to set 10.10.10.0 255.255.255.128 as the cluster management IP address pool.

```
CLUSTER_1.Ruijie(config-cluster)#     management     ip-pool     10.10.10.0
255.255.255.128
```

Related Commands

Command	Description
show cluster	Show basic information about the cluster that the device belongs to.
show cluster candidates	Show information about a candidate device.
show cluster member	Show information about a member device.
show cluster topology	Show topology information about the cluster.

Platform Description

N/A

member add

Add a specified candidate device to the cluster. Use the **no** form of this command to delete a static member device.

member add [*member-id*] **mac-address** *H.H.H*

no member add *member-id*

Parameter Description

Parameter	**Description**
H.H.H	MAC address of a candidate device
member-id	SN of the cluster to which the device is added. When the subnet mask of the cluster management IP address contains no more than 24 digits, the cluster SN range is 2 to 240. When the subnet mask of the cluster management IP address contains more than 24 digits, for example 255.255.255.128: The allocable IP host number range is 2 to 126, excluding IP host numbers consists of only zeros or all ones, and the one assigned to the management device; The allocable cluster SN range is 2 to126.

Defaults None.

Command Mode Cluster configuration mode

Usage Guide Use this command to add a specified candidate device as a static member to the cluster.

Use the **no** form of this command to delete a static member device from the cluster.

Caution

This command fails to be used if the specified *member-id* has been assigned to another device.

The **no** form of this command can be used to delete only member devices added through the **member add** command. That is, the device SN property must be static. If the **member auto-add** function of the cluster is enabled, the cluster re-adds the deleted member to the cluster. At this time, the member device SN property is dynamic.

Note

The SN property can be static or dynamic. If the property is static, this command can be used to configure the cluster management SN for the device, and another device cannot use the SN even when the device is a candidate device or off the network. If the property is dynamic, the cluster automatically discovers a candidate device, adds it as a member device, and assigns an SN to a device when the **member auto-add** function is enabled. When the device exits the network or becomes a candidate device, the cluster reclaims the SN and assigns it to another device.

After this command is used for a specified candidate device, the cluster assigns a cluster SN and adds the device as a static member. If no *member-id* is specified, the cluster automatically obtains an idle SN for the device.

.Use this command to change the assigned cluster SN when the member device is specified. If no *member-id* is specified, only the attribute of the assigned SN is changed to "static".

If the **no** form of this command is used to delete a member device, the management device changes the SN property to "dynamic", holds the SN for a period, and then releases it.

Configuration Examples

Example 1: Use the following command to add the device with the MAC address 00d0.f8fe.1007 to the cluster and specify the cluster SN as 2:

```
CLUSTER_1.Ruijie(config-cluster)#member add 2 mac-address 00d0.f8fe.1007
```

Related Commands

Command	Description
member auto-add	Add all candidate devices as members and automatically add latterly discovered devices as members.
member black-list	Prohibit adding blacklisted devices as members.
member password	Add a member device configured with a password. Addition succeeded only when rules configured in the password are met.
show cluster	Show basic information about the cluster that the device belongs to.
show cluster candidates	Show information about a candidate device.
show cluster member	Show information about a member device.
show cluster topology	Show topology information about the cluster.

Platform Description

N/A

member auto-add

Add all candidate devices in the cluster as members and automatically add latterly discovered devices to the cluster as members. Use the **no** form of this command to disable the **member auto-add** function.

member auto-add

no member auto-add

Parameter Description

Parameter	Description
-	-

Defaults

Enabled

Command Mode

Cluster configuration mode

Usage Guide

Add all candidate devices in the cluster, so that these devices become cluster members.

After this command is configured, latterly discovered devices will also be automatically added to the cluster and become members.

The **no** form of this command can be used to disable the **member auto-add** function, but the system asks you whether to transform existing dynamic members into static members. If yes, the dynamic members are transformed into static members. If no, all existing dynamic members are deleted.

Caution

Devices that are blacklisted or without the cluster function cannot become member devices.

If the **member auto-add** function is disabled, all dynamic members are deleted by default.

Note

If the **member auto-add** function is enabled, you can blacklist the member device or disable its cluster function for fundamentally deleting the member device.

If the **no** form of this command is used and you choose **NO**, the management device deletes all dynamic members, holds the SN for a period, and then releases it.

Configuration Examples

Example 1: Use the following command to add all candidate devices in the cluster as members:

```
CLUSTER_1.Ruijie(config-cluster)#member auto-add
```

Related Commands

Command	Description
member add	Add a specified device to the cluster.
member black-list	Prohibit adding blacklisted devices as members.
member password	Add a member device configured with a password. Addition succeeded only when rules configured in the password are met.
show cluster	Show basic information about the cluster that the device belongs to.
show cluster candidates	Show information about a candidate device.
show cluster member	Show information about a member device.

Platform Description

N/A

member black-list

Add the device with a specified MAC address to the cluster blacklist. Use the **no** form of this command to delete a blacklist.

member black-list *H.H.H*

no member black-list { *H.H.H* }

Parameter Description

Parameter	Description
H.H.H	MAC address of the device to be blacklisted.

Defaults

No device is blacklisted.

Command Mode

Cluster configuration mode

Usage Guide

Use the **member black-list** *H.H.H* command to add the device with a specified MAC address to the cluster blacklist. That is, prohibit the device being added to the cluster. You can specify the device, including a device that is not connected to the network, at your will. If the specified device is in the cluster topology table, the device and its associated devices will exit the cluster and the device is blacklisted.

Use the **no member black-list** *H.H.H* command to delete a specified device from the blacklist.

Use the **no member black-list** command to delete the entire blacklist. After the device is deleted from the blacklist, it can join a cluster and become a member device.

⚠ Caution

When *H.H.H* specifies the cluster management device, the command is invalid.

Blacklisted devices do not forward packets. Therefore, devices associated with the blacklisted devices will not be discovered by the management device.

Configuration Examples

Example 1: Add the device with the MAC address 0010-3500-e001 to the blacklist.

```
CLUSTER_1.Ruijie(config-cluster)#member black-list 0010-3500-e001
```

Example 2: Release all devices in the current cluster blacklist.

```
CLUSTER_1.Ruijie(config-cluster) #no member black-list
```

Related Commands

Command	Description
member add	Add a specified device to the cluster.
member auto-add	Add all candidate devices to the cluster.
show cluster candidates	Show information about a candidate device.
show cluster topology	Show topology information about the cluster.
show cluster black-list	Show all the blacklist information.

Platform Description

N/A

member password

Configure the authentication password of privileged EXEC mode for the management device or configure the authentication password for a specified device. Use the **no** form of this command to delete the authentication password.

member password { *password-id* **|** *H.H.H* } { *password* **|** *encryption-type encrypted-password* }

no member password { *password-id* | *H.H.H*}

Parameter Description

Parameter	Description
password-id	Password SN of the cluster management
H.H.H	MAC address of the device
password	Plain text password
encryption-type	Encryption mode of the authentication password. **0**: not encrypted; **7**: encrypted.
encrypted-password	Authentication password after the encryption mode is specified

Defaults

None

Command Mode

Cluster configuration mode

Usage Guide

Use the **member password** *password-id* command to configure the authentication password of privileged EXEC mode for the management device. The password pool allows a maximum of 16 passwords. Use the **no** form of this command to delete the authentication password with the password pool SN being *password-id.*

Use the **member password** *H.H.H* command to configure the authentication password for a specified device. Use the **no** form of this command to delete the authentication password of the specified device.

⚠ Caution

If a candidate device is configured with a password, the cluster needs to perform authentication when adding the device. Addition succeeds only when the authentication passes.

After a member device joins the cluster, the management device re-performs authentication if the password is changed. If authentication fails, the member device exits the cluster.

Note

When the cluster adds a member device, authentication is performed based on the authentication password. The default authentication sequence is as follows: **member password** *H.H.H*; **member password** *password-id*; Password of the management device; Null password. Member device addition fails only when all the preceding passwords fail to be authenticated.

Configuration Examples

Example 1: Use the following command to configure the plaintext password aaa for the device with the MAC address 00d0.f8fe.1007:

```
CLUSTER_1.Ruijie(config-cluster)#member password 00d0.f8fe.1007 aaa
```

Example 2: Use the following command to add the plaintext password bbb to the cluster authentication password pool and specify the cluster SN to 12:

```
CLUSTER_1.Ruijie(config-cluster)#member password 12 bbb
```

Related Commands

Command	**Description**
member add	Add a specified device to the cluster.
member auto-add	Add all candidate devices as members and automatically add latterly discovered devices as members.
show cluster	Show basic information about the cluster that the device belongs to.
show cluster candidates	Show information about a candidate device.
show cluster member	Show information about a member device.
show cluster topology	Show topology information about the cluster.

Platform Description

N/A

proxy tftp-server

Set the cluster-sharing TFTP server. Use the **no** form of this command to delete the set TFTP server address.

proxy tftp-server *ip-address*

no proxy tftp-server

Parameter Description

Parameter	**Description**
ip-address	IPv4 address of the cluster-sharing TFTP servers

Defaults

No cluster-sharing TFTP server is set.

Command Mode Cluster configuration mode

Usage Guide Use this command to set the cluster-sharing TFTP server, so that a member device can use the TFTP agent service of the management device to upload or download files from the specified TFTP server when the there is no public network IP address configured for the member device.

Configuration Examples Example 1: Use the following command to set the TFTP server with the address 172.10.1.1 as the cluster-sharing TFTP server:

```
CLUSTER_1.Ruijie(config-cluster)# proxy tftp-server 172.10.1.1
```

Related Commands

Command	Description
cluster tftp	Cluster TFTP agent
show cluster	Show basic information about the cluster that the device belongs to.

Platform Description N/A

show cluster

Show basic information about the cluster that the device belongs to.

show cluster

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Privileged EXEC mode

Usage Guide Show basic information about the cluster.

Note

Use this command on the management device to show the cluster name, cluster SN of the management device, MAC address of the management device, management device name, cluster management information, member count, cluster status, operation time, and related configurations.

Use this command on a member device to show the cluster name, cluster SN of the member device, MAC address of the management device, management device name, and cluster management resources.

Configuration Examples

Example 1: Show basic information about the cluster on the management device.

```
CLUSTER_1.Ruijie#show cluster
Cluster:                    CLUSTER<Administrator>
Member-id:                   1
Administrator mac address:    00d0.f822.33ac
Administrator name:          ruijie
Management vlan:             2056
Management ip:              192.168.176.1
Management ip-pool:           192.168.176.0/24
Total number of members:      2
Status:                     0 members are unreachable
Run time:                    0 days, 1 hours, 5 minutes, 37 seconds
Timer:                      60 seconds
Timer hello:                 30 seconds
Timer hold:                  90 seconds
Hops-limit:                  5
Proxy tftp-server:            Not configured!
```

Example 2: Show basic information about the cluster on a member device.

```
CLUSTER_2.Ruijie#show cluster
Cluster:                    CLUSTER<Member>
Member-id:                   2
Administrator mac address:    00d0.f822.33ae
Administrator name:          Ruijie
Management vlan:             2049
Management ip:              192.168.176.2
```

Field	Description
Cluster	Name and role of the cluster
Member-id	Management device SN
Administrator mac address	MAC address of the management device
Administrator name	Host name of the management device
Management vlan	Cluster management VLAN
Management ip	IP address assigned to cluster devices
Management ip-pool	IP address used in cluster management
Total number of members	Number of cluster members, including the management device and member devices
Status	Status of a cluster member
Run time	Cluster operation time
Timer	Cluster timer value
Timer hello	Cluster timer-hello value
Timer hold	Cluster timer-hold value

Hops-limit	Cluster hop count range
Proxy tftp-server	Address of the TFTP servers shared by clusters

Related Commands

Command	Description
cluster	Create a cluster.
cluster enable	Enable the cluster function for the device.

Platform Description

N/A

show cluster black-list

Show all the blacklist information.

show cluster black-list

Parameter Description

Parameter	Description
-	-

Defaults

-

Command Mode

Privileged EXEC mode

Usage Guide

Caution

The command can be used only on the management device to show the related information.

Configuration Examples

Example 1: Show all the blacklist information on the management device.

```
CLUSTER_1.Ruijie #show cluster black-list
MAC            Hops LcPort    UpSN      UpMAC         UpPort
-------------- ---- --------- ---- -------------- ---------
00d0.f8fe.43d2 1    Fa0/2     1    00d0.f8fe.1007  Fa0/3
00d0.f8fe.a861 -    -         -    -               -
```

Field	Description
MAC	MAC address of a blacklisted device if the device is on the network
Hops	Topology hop count from a blacklisted device to the management device if the blacklisted device is on the network

LcPort	Port on a blacklisted device, connecting a blacklisted device to its associated device if the blacklisted device is on the network
UpSN	Cluster SN of an associated device if it is a member device
UpMAC	MAC address of an associated device if it is a member device
UpPort	Port on an associated device, connecting the associated device to a blacklisted device if the associated device is on the network

Related Commands

Command	Description
cluster	Create a cluster.
member black-list	Prohibit adding blacklisted devices as members.

Platform Description N/A

show cluster candidates

Show information about a candidate device.

show cluster candidates [**detail** | *H.H.H*]

Parameter Description

Parameter	Description
detail	Show details about all the candidate devices.
H.H.H	Indicate the MAC address of a specified candidate device.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide Use the **show cluster candidates** command to show information about all the candidate devices.

Use the **show cluster candidates detail** command to show details about all the candidate devices.

Use the **show cluster candidates** *H.H.H* command to show details about a specified candidate device.

Caution

This command can be used only on the management device to show the related information.

Configuration Example 1: Show information about a candidate device on the management device.

Examples

```
CLUSTER_1.Ruijie#show cluster candidates
MAC            Hops LcPort    UpSN      UpMAC       UpPort    STATUS
-------------- ---- --------- ---- -------------- --------- ------
00d0.f8fe.43d2 1    Fa0/2     1    00d0.f8fe.1007  Fa0/3    ready
00d0.f8fe.a861 2    Fa0/5     -    00d0.f8fe.43d2  Fa0/12   ready
```

Field	Description
MAC	MAC address of a candidate device
Hops	Topology hop count from a candidate device to the cluster management device
LcPort	Port on a candidate device, connecting the candidate device to an associated device
UpSN	Cluster SN of an associated device if it is a member device
UpMAC	MAC address of an associated device
UpPort	Port on an associated device, connecting the associated device to a candidate device
STATUS	Status of the cluster. The value can be READY or INVALID. The cluster is in the INVALID state when the cluster management function is disabled on the device or the device is blacklisted.

Related Commands

Command	Description
cluster	Create a cluster.
cluster member	Add a member device to the cluster.
cluster enable	Enable the cluster function for the device.

Platform Description N/A

show cluster member

Show information about a member device.

show cluster members [*member-id* | **detail**]

Parameter Description

Parameter	Description
member-id	Indicate the cluster SN of a member device.
detail	Show details about all the member devices.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide

Use the **show cluster members** command to show details about all the member devices.

Use the **show cluster members** *member-id* command to show details about a member device with a specified SN.

Use the s**how cluster members detail** command to show details about all the member devices.

Caution

The command is invalid if it is run on a candidate device. On a member device, information is shown only when the **show cluster members** command is run. In addition, the shown information involves only the member device itself and the management device.

Configuration Examples

Example 1: Show information about a member device on the management device.

```
CLUSTER_1.Ruijie #show cluster members
SN        MAC       Name       Hops State   LcPort    UpSN      UpMAC     UpPort
---- -------------- ----------- ---- ------- --------- ---- --------------
---------
1    00d0.f8fe.1007 Ruijie     0    <Admin>
2    00d0.f8fe.43d2 Ruijie     1    up      Fa0/2     1    00d0.f8fe.1007 Fa0/3
3    00d0.f8fe.a861 Ruijie      2    up      Fa0/5      2    00d0.f8fe.43d2
Fa0/12
```

Example 2: Show details about a member device on the management device.

```
CLUSTER_1.Ruijie #show cluster member detail
Device 'switch-1' with member id 2 (Member)
       Device type:              S2628G
       MAC address:              00d0.f8fe.43d2
       Serial Number:            1234942576719
       Upstream MAC address:       00d0.f8fe.1007
       Local port:               Fa0/2
       Upstream port:            Fa0/3
       Hops from Administrator:    1
       Last topo update:          37 seconds ago
       Last udp update:           7 seconds ago
       Management ip:            192.168.176.2
       State:                   up (Active)
       no receive topo respone:    0 times
       no receive udp respone:     0 times
       add method:               Manually add
Device 'switch-2' with member id 3 (Member)
       Device type:              S2628G
       MAC address:              00d0.f8fe.a861
       Serial Number:            1234942571123
       Upstream MAC address:       00d0.f8fe.43d2
       Local port:               Fa0/5
       Upstream port:             Fa0/12
       Hops from Administrator:    2
       Last topo update:          37 seconds ago
       Last udp update:           7 seconds ago
       Management ip:             192.168.176.3
       State:                    up (Active)
       no receive topo respone:    0 times
       no receive udp respone:     0 times
       add method:                Manually add
```

Example 3: Show information about member device 0 on member device 2.

```
CLUSTER_2.Ruijie #show cluster members
SN      MAC       Name      Hops State    LcPort   UpSN     UpMAC    UpPort
---- -------------- ---------- ---- -------- --------- ---- -------------
---------
1   00d0.f8fe.1007 Ruijie    0   <Admin>
2    00d0.f8fe.a861  Ruijie     2    up       Fa0/5     1    00d0.f8fe.43d2
Fa0/12
```

Field	Description
SN	Cluster SN of a device
MAC	MAC address of a member device
Name	Host name of a member device
Hops	Topology hop count from a member device to the management device
State	Status of a member device. The value can be: up: indicates that the device is valid; down: indicates that the device is lost < Admin>: indicates that the device is the management device.
LcPort	Port on a member device, connecting the member device to an associated device
UpSN	Cluster SN of an associated device if it is a member device
UpMAC	MAC address of an associated device
UpPort	Port on an associated device, connecting the associate device to a member device

Related Commands

Command	Description
cluster	Create a cluster.
member add	Add a specified device to the cluster.
member auto-add	Add all candidate devices to the cluster.

Platform Description

N/A

show cluster topology

Show topology information about the cluster.

show cluster topology [*H.H.H* **|** *member-id*]

Parameter Description

Parameter	Description
H.H.H	MAC address of a specified cluster device
member-id	Cluster SN of a member device

Defaults

-

Command Mode

Privileged EXEC mode

Usage Guide

Use the **show cluster topology** command to show the topology information about the cluster.

Use the **show cluster topology** *H.H.H* command to show the topology information associated with the root node specified in *H.H.H.*

Use the **show cluster topology** *member-id* command to show the topology information associated with the root node specified in *member-id.*

Caution

This command can be used only on the management device to show the related information.

Configuration Examples

Example 1: Show topology information about the cluster on the management device.

```
CLUSTER_1.Ruijie#show cluster topology
----------------------------------------------------------------------
   (PeerPort) ConnectFlag (LocalPort) [HostName:DeviceMac]
----------------------------------------------------------------------
ConnectFlag:
   <--> normal connect   **** cluster unenable  -||- in blacklist
   ???? status down
----------------------------------------------------------------------
[CLUSTER_1.Ruijie:00d0.f822.33c8]
   |
   +--(Fa0/11) <--> (Fa0/13)[CLUSTER_3.Ruijie:001a.a97b.d3ac]
   |   |
   |   +--(Fa0/23) <--> (Fa0/21)[CLUSTER_4.ruijie:001a.a97e.043b]
   |      (Fa0/7) <--> (Fa0/7)
   |
   +--(Fa0/3) <--> (Fa0/4)[CLUSTER_2.ruijie:001a.a908.7a7e]
```

Example 2: Show the network topology information associated with member device 3 on the management device.

```
CLUSTER_1.Ruijie#show cluster topology 3
---------------------------------------------------------------------
   (PeerPort) ConnectFlag (LocalPort) [HostName:DeviceMac]
---------------------------------------------------------------------
ConnectFlag:
   <--> normal connect   **** cluster unenable  -||- in blacklist
   ???? status down
---------------------------------------------------------------------
[CLUSTER_3.Ruijie:001a.a97b.d3ac]
   |
   +--(Fa0/23) <--> (Fa0/21)[CLUSTER_4.ruijie:001a.a97e.043b]
      (Fa0/7) <--> (Fa0/7)
```

Field	Description
PeerPort	Port of a neighbor
ConnectFlag	Connection flag
LocalPort	Port of a local device
HostName	Name of a device. If the device has joined the cluster, its name contains the cluster prefix such as CLUSTER_4.
DeviceMac	MAC address of a device
<-->	The symbol indicating that the device is properly connected to the management device
****	Cluster function is disabled on the device. That is, the no cluster enable command is run.
-||-	The symbol indicating that the device is blacklisted
????	The symbol indicating that the member device is in the down state

Related Commands

Command	Description
cluster	Create a cluster.
cluster explore	Run the command on the management device to manually start topology collection.

Platform Description

N/A

timer

Set the cluster timer. Run the **no** form to restore the default value.

timer { *topo-seconds* **| hello** *hello-seconds* **| hold** *hold-seconds* }

no timer [*topo-seconds* | **hello** *hello-seconds* **| hold** *hold-seconds*]

Parameter Description

Parameter	Description
topo-seconds	Set the cluster topology collection timer. The range is 10 to 300 and the unit is second.
hello-seconds	Set the update time of the member device status. The range is 10 to 300 and the unit is second.
hold-seconds	Set the hold time of the member device status. The range is 10 to 300 and the unit is second.

Defaults

timer: 60 seconds
timer-hello: 30 seconds
timer-hold: 90 seconds

Command Mode

Cluster configuration mode

Usage Guide

To improve the topology convergence, adequately decrease the value of **timer** *topo-seconds.* If the network is stable, it is recommended to increase the value to reduce the packet traffic in the network.

Configuration Examples

Example 1: Run the following command to set the topology collection time to 80 seconds:

```
CLUSTER_1.Ruijie(config-cluster)#timer 80
```

Example 2: Run the following command to set the member status hold time to 95 seconds:

```
CLUSTER_1.Ruijie(config-cluster)#timer hold 95
```

Related Commands

Command	Description
show cluster	Show basic information about the cluster that the device belongs to.

Platform Description

N/A

Device Redundancy Configuration Commands

auto-sync

Use this command to synchronize runing-config and startup-config in the case of redundancy of dual supervisor engines. Use the **no** form of this command to disable the function.

auto-sync { **standard | running-config | startup-config}**

no auto-sync { **standard | running-config** | **startup-config**}

Parameter description

Parameter	Description
standard	Synchronize all the system files.
running-config	Synchronize the runtime configuration files.
startup-config	Synchronize the startup configuration files.

Default

All the files are synchronized by default.

Command mode

Redundancy configuration mode.

Usage guidelines

Generally the standard synchronization should be used if there is no special requirement.

Examples

The following example only synchronizes the startup-config files

```
Ruijie(config)# redundancy
Ruijie(config-red)# auto-sync startup-config
Ruijie(config-red)# exit
```

The following example synchronizes all the files other than the starup-config files.

```
Ruijie(config)# redundancy
Ruijie(config-red)# no auto-sync startup-config
Ruijie(config-red)# exit
```

Platform description

N/A

auto-sync time-period

Use this command to configure the auto-sync time-period of runing-config and startup-config when the dual supervisor engines is redundant. Use the **no** form of this command to disable the function.

auto-sync time-period *value*

no auto-sync time-period

Parameter description

Parameter	Description
value	Auto-sync time-period interval (second).

Default

Auto-sync with 1 hour (3600 seconds) time-period interval

Command mode

Redundancy configuration mode.

Usage guidelines

Use standard synchronization if there is no particular demand.

Examples

The following example only synchronizes the startup-config file:

```
Ruijie(config)# redundancy
Ruijie(config-red)# auto-sync time-period 60
Redundancy auto-sync time-period: enabled (60 seconds). Ruijie(config-red)#
exit
```

The following example disables auto-sync:

```
Ruijie(config)# redundancy
Ruijie(config-red)# no auto-sync time-period
Redundancy auto-sync time-period: disabled. Ruijie(config-red)# exit
```

Platform description

N/A

redundancy

Use this command to enter redundancy configuration mode in the global configuration mode.

Redundancy

Command mode

Global configuration mode.

Usage guidelines

Enter the redundancy configuration mode in the global configuration mode to execute the redundant mode commmands like auto-sync, auto-sync time-period, switchover timeout,etc, to do the related redundancy configuration.

Examples

```
Ruijie# config terminal
Ruijie(config)# redundancy
Ruijie(config-red)# exit
```

Platform description N/A

redundancy reload

In the privileged EXEC mode, use the **redundancy reload** command to reset slave device or reset both master and slave devices.

redundancy reload {**peer** | **shelf** [*switchid*]}

Parameter description

Parameter	Description
peer	Reset the slave device only.
shelf	Reset the master and slave devices in the standalone mode. In the VSU mode, the ID of the switch to be reset must be specified.
switchid	VSU switch ID. This parameter is supported in the VSU mode. Currently the value ranges from 1 to 8.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines

The redundancy reload peer does not affect the data transfer. During the resetting of the Slave, the data transfer is not disconnected and the user session information is not lost.

In the VSU mode, the command is redundancy reload shelf *switched*. This command resets a specified switch.

Examples

```
Ruijie# redundancy reload peer
This operation will reload the current standby unit which is inserted in slot
M2. Are you sure to continue? [N/y] y
Preparing to reload peer
```

Related commands

Command	Description
reload	Reset the master supervisor engine.

Platform description N/A

redundancy forceswitch

In privileged EXEC mode, use this command to enforce Slave supervisor engine to switchover.

redundancy forceswitch

Parameter description

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command allows you to select the slot in which the supervisor engine serves as the master supervisor engine and that as the slave supervisor engine, or the slot in which the supervisor engine is superior to that in another slot as the master board.

Examples

```
Ruijie# redundancy forceswitch

This operation will reload the active unit and force switchover to the standby
unit which is inserted in slot M1. Are you sure to continue? [N/y] y
```

Related commands

Command	Description
reload	Reset the master supervisor engine.

Platform description

N/A

switchover timeout

In the redundancy configuration mode, use the **switchover timeout** command to configure the switchover timeout value for the supervisor engine. Use the **no** form of this command to restore the timeout to the default value.

switchover timeout *timeout-period*

no switchover timeout

Parameter description

Parameter	Description
timeout-period	Switchover timeout in the range 160 to 25,000 (milliseconds).

Default

4000 milliseconds.

Command mode

Redundancy configuration mode.

Usage guidelines

When the slave device has not received a heartbeat message of the master device within the timeout period, the switchover will occur. If you are not sure, do no modify the default value.

Examples

```
Ruijie# config terminal
Ruijie(config)# redundancy
Ruijie(config-red)#
Ruijie(config-red)# switchover timeout 4000
Ruijie(config-red)# exit
Ruijie(config)# exit
Ruijie(config)#
```

Platform description N/A

show redundancy auto-sync

Use command **show redundancy auto-sync** to show the current redundancy auto-sync mode in user EXEC or privileged EXEC mode. For the detailed information, please refer to auto-sync description in previous text.

show redundancy auto-sync

Default N/A

Command mode User mode or Privileged EXEC mode.

Examples

```
Ruijie> enable
Ruijie# show redundancy auto-sync
Redundancy auto-sync mode: auto-sync standard.
...
```

Platform description N/A

show redundancy states

Use this command to show the current redundancy in the user mode or privileged EXEC mode.

show redundancy states

Parameter description

Parameter	Description
states	Show the redundancy status of the master or the slave devices.

Default N/A.

Command mode User mode or privileged EXEC mode

Usage guidelines Currently, only 1:1 hot backup (for the global master board and slave board) is supported in the VSU mode. Therefore, only the hot backup state of the local and peer device is displayed.

Examples

```
Ruijie> enable
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie# show redundancy states
Redundancy states:
My state = 19 -ACTIVE
peer state = 37 -STANDBY HOT
...
```

Platform description N/A

show redundancy switchtimeout

Use **show redundancy switchtimeout** command to show current redundanct switchover timeout time in user EXEC or privileged EXEC mode.

show redundancy switchtimeout

Default N/A

Command mode User mode or Privileged EXEC mode.

Examples

```
Ruijie> enable
Ruijie# show redundancy switchtimeout
redundancy switch timeout is : 4000 ms.
...
```

Platform description N/A

SRM Configuration Commands

cpu

In the srm-policy configuration mode, use this command to enter the owner-cpu configuration mode.

cpu

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode srm-policy configuration mode

Usage Guide N/A

Configuration Examples Example 1: In the srm-policy configuration mode, execute "cpu" command to enter the owner-cpu configuration mode.

```
Ruijie(config-srm-policy)#cpu
Ruijie(config-owner-cpu)#
```

Related Commands

Command	Description
resource manager	Enter the SRM configuration mode.
policy *policy-name* [**global**]	Create the monitoring policy and enter the SRM-policy configuration mode.

Platform Description N/A

instance

In the config-res-group configuration mode, use this command to add resource users into the group.

instance *resource-user_name*

no instance *resource-user_name*

Parameter Description

Parameter	Description
resource-user_name	Name of resource user. Execute "show resource database"

	command to display the information about resource users.
no	Remove resource user from the group.

Defaults N/A

Command Mode SRM configuration mode.

Usage Guide N/A

Configuration Examples Example 1: Configure a resource user group named rgos_group and add the snmpd into the group, and finally apply the monitoring policy to the group.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#user group rgos_group
Router(config-res-group)#instance snmpd
```

Related Commands

Command	Description
resource manager	Enter the SRM configuration mode.

Platform Description N/A

memory

In the srm-policy configuration mode, use this command to enter the owner-memory configuration mode.

memory

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Srm-policy configuration mode

Usage Guide N/A

Configuration Examples Example 1: In the srm-policy configuration mode, use the **memory** command to enter the owner-memory configuration mode.

```
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#
```

Related Commands

Command	Description
resource manager	Enter the SRM configuration mode.
policy *policy-name* [**global**]	Create the monitoring policy and enter the SRM-policy configuration mode.

Platform Description

N/A

policy

In the srm configuration mode, use this command to create the monitoring policy and enter the srm-policy configuration mode.

policy *policy-name* [**global**]

no policy *policy-name*

Parameter Description

Parameter	Description
policy-name	Policy-name: name of policy.
global	If you add the global parameter, it will become a global monitoring policy; otherwise, it is a user monitoring policy.
no	Remove the monitoring policy.

Defaults

N/A

Command Mode

SRM configuration mode.

Usage Guide

N/A

Configuration Examples

Example 1: Configure a global monitoring policy named rgos_policy.

```
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy global
Ruijie(config-srm-policy)#
```

Example 2: Configure a user monitoring policy named rgos_policy.

```
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy
Ruijie(config-srm-policy)#
```

Related Commands

Command	Description
resource manager	Enter the SRM configuration mode.

Platform Description N/A

policy *policy-name*

In the config-res-group configuration mode, use this command to associate the group with monitoring policy.

policy *policy-name*

no policy *policy-name*

Parameter Description

Parameter	Description
policy-name	Name of monitoring policy.
no	Remove the association between group and monitoring policy.

Defaults N/A

Command Mode SRM configuration mode.

Usage Guide N/A

Configuration Examples Example 1: Configure a group named rgos_group and add snmpd into the group, and finally apply the policy to this group.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#user group rgos_group
Router(config-res-group)#instance snmpd
Router(config-res-group)#policy rgos_policy
```

Related Commands

Command	Description
resource manager	Enter the SRM configuration mode.

Platform Description N/A

resource manager

Enter the SRM configuration mode in global mode.

resource manager [**slot** *slot-id* [**subsystem** *subsystem-id*]]

Parameter

Parameter	Description

Description

slot *slot-id*	Specify the board card to be configured.
subsystem *subsystem-id*	Subsystem id (range: 0-1), equivalent to the cpu id displayed after executing "show version" command.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples Example: Enter the SRM configuration mode.

```
Ruijie(config)#resource manager
Ruijie(config-srm)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

rising

In the owner-memory or owner-cpu configuration mode, use this command to configure monitoring waterlines.

{ **critical** | **major** | **minor** } **rising** *rising-waterline-value* [**interval** *interval-value*] [**falling** *falling-waterline-value* [**Interval** *interval-value*]]

no { **critical** | **major** | **minor** }

Parameter Description

Parameter	Description
rising	Rising waterline.
rising-waterline-value	Rising waterline value (unit: percent; range: 1-100).
interval-value	Holding time, with unit being second, minimal value being 5s and maximal value being 86400s (24 hours).
falling	Falling waterline.
falling-waterline-value	Falling waterline value (1-100); the falling value must be less than the rising value.
no	Remove the waterline.

Defaults N/A

Command Mode

owner-memory or owner-cpu configuration mode

Usage Guide

Caution

The rising waterline of major must be greater than that of minor, and the rising waterline of critical must be greater than that of major.

Configuration Examples

Example 1: Configure critical waterline.

```
Ruijie(config-srm-policy)#memory
Ruijie(config-owner-memory)#critical rising 80 falling 15 interval 10
```

Related Commands

Command	Description
resource manager	Enter the SRM configuration mode.
policy *policy-name* [**global**]	Create the policy and enter the SRM-policy configuration mode.
memory	Enter the owner-memory configuration mode.
cpu	Enter the owner-cpu configuration mode.

Platform Description

N/A

show resource database

Display the SRM database information, including information about resource owner, resource user group and resource users.

show resource database [**slot** *slot-id* [**subsystem** *subsystem-id*]]

Parameter Description

Parameter	Description
slot *slot-id*	Specify the board card to be displayed.
subsystem *subsystem-id*	Subsystem id (range: 0-1), equivalent to the cpu id displayed after executing "show version" command.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Example 1: Display the information of all SRM databases.

```
Ruijie#show resource database
```

```
Resource Owners            ID
----------------------------------------------------------------
Cpu                            0x0
Memory                         0x1

Resource Users             ID              Priority
----------------------------------------------------------------
Ktimer                         0x1             PROT_TASK
Atimer                         0x2             APP_TASK
printk_task                0x3             APP_TASK_TS
waitqueue_process           0x4            PROT_TASK
tasklet_task               0x5         PROT_TASK
cmic_pause_detect           0x6            PROT_TASK
idle                           0x7             IDLE
kevents                    0x8             PROT_TASK
snmpd                      0x9             PROT_TASK
snmp_trapd                     0xa             APP_TASK
mtdblock                   0xb             PROT_TASK
gc_task                    0xc             PROT_TASK
Context                    0xd             PROT_TASK
kswapd                         0xe             PROT_TASK
--More—
```

Field	Description
Resource Owners	Resource owner
ID	Identifier
Resource User Groups	Resource user group
Resource Users	Resource user
Priority	Task priority, divided into: PROT_TASK: core thread HAPP_TASK_TS: high priority user thread APP_TASK: application thread APP_TASK_TS: application thread with time slice IDLE: exclusive for idle process

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show resource notification

Display statistics of SRM monitoring event notifications.

show resource notification owner { **all | cpu | memory** } [**slot** *slot-id* [**subsystem** *subsystem-id*]]

Parameter Description

Parameter	Description
all	Statistics of all ROs.
cpu	Statistics of CPU.
memory	Statistics of memory.
slot *slot-id*	Specify the board card to be displayed.
subsystem *subsystem-id*	Subsystem id (range: 0-1), equivalent to the cpu id displayed after executing "show version" command.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples Example 1: Display statistics of all SRM monitoring notifications.

```
Ruijie#show resource notification owner all
Owner: cpu

Global                  Global Notif.(cr(U/D):ma(U/D):mi(U/D))
-------------------------------------------------------------
global                             Not in monitored



Multi-User Group        User Notif.(cr(U/D):ma(U/D):mi(U/D))
-------------------------------------------------------------
rgnos_group                         (cr(0/0):ma(0/0):mi(0/0))



Single-User Group       User Notif.(cr(U/D):ma(U/D):mi(U/D))
-------------------------------------------------------------
ktimer                             (cr(0/0):ma(0/0):mi(0/0))



Owner: memory

RU Global                  Global Notif.(cr(U/D):ma(U/D):mi(U/D))
---------------------------------------------------------------
```

```
global                            Not in monitored



Multi-User Group         User Notif.(cr(U/D):ma(U/D):mi(U/D))
---------------------------------------------------------------
rgnos_group                        (cr(0/0):ma(0/0):mi(0/0))



Single-User Group        User Notif.(cr(U/D):ma(U/D):mi(U/D))
---------------------------------------------------------------
ktimer                            (cr(0/0):ma(0/0):mi(0/0))
```

Field	Description
Global	Global resource usage
Multi-User Group	Multi-user resource user group
Single-User Group	Single-user resource user group
Global Notif.	Notifications of global policy monitoring waterline
User Notif.	Notifications of user policy monitoring waterline
cr(U/D):ma(U/D):mi(U/D)	Times of passing critical, major and minor waterlines; U refers to UP event notification; D refers to DOWN event notification.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show resource owner

Display information about SRM resource owner.

show resource owner { **all** **|** **cpu** **|** **memory** } [**slot** *slot-id* [**subsystem** *subsystem-id*]]

Parameter Description

Parameter	Description
all	Information about all SRM resource owners.
cpu	Information about CPU owner.
memory	Information about memory owner.
slot *slot-id*	Specify the board card to be displayed.
subsystem *subsystem-id*	Subsystem id (range: 0-1), equivalent to the cpu id displayed after executing the **show version** command.

Defaults

N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples Example 1: Display SRM resource usage status.

```
Ruijie#show resource owner all
Resource Owner: CPU
Used Ratio(%): 5Sec -- 93, 1Min -- 93, 5Min – 93

RU Group                   Runtime(ms) 5Sec        1Min        5Min
----------------------------------------------------------------
rgnos_group            1590380         0         0         0

RU                         Runtime(ms) 5Sec        1Min        5Min
----------------------------------------------------------------
rl_con                 171420          0           0           0
stat_get_and_send      1585180    1           1           1
cmic_pause_detect      1585180    0           0           0
mem_info_task              1602670        0           0           0
idle_vlan_proc_thread      1602670        0         0         0
rerp_msg_recv_thread       1602760    0         0         0
ssp_mc_trap_task           1602920    0         0         0
ssp_flow_rx_task           1604410    0           0           0
flow_warn_msg_task         1604440        0           0           0
flow_age_task              1604440    0           0           0
temperature_handler_task   1604650    0         0         0
keepalive_link_notify      1604700        0         0         0
datapkt_rcv_thread         1604700        0         0         0
rdp_slot_change_thread 1604700        0         0           0
printk_task            2172590    92          92          92
idle                       2172590    7           7         7

Resource Owner: memory
Total Size(B): 536870912
Used  Size(B): 143081472
Used  Ratio(%): 27

RU Group               Allocated Size(B)       Alloc Cnt   Free Cnt
---------------------------------------------------------------
local-1             0                      0       0

RU                     Allocated Size(B)       Alloc Cnt   Free Cnt
---------------------------------------------------------------
```

```
Ktimer                  0                      7065        14
atimer              92                     2343        3
printk_task         0                      0           0
waitqueue_process       0                      0       0
tasklet_task            2656                   21      4
idle                    0                      0       0
ttipc_timer         0                      1610        1610
kevents             0                      0       0
iftp_server         0                      0           0
snmpd                   45312              53      47
snmp_trapd              0                      0           0
mtdblock                0                      0           0
gc_task             4                      13          13
context             0                      0           0
kswapd              0                      0           0
bdflush             0                      0           0
kupdate                 0                      2           2
```

Field	Description
Total Size(B)	Total memory size (byte)
Used Size(B)	Used memory size (byte)
Used Ratio(%)	Resource utilization.
RU Group	Resource user group
RU	Resource user
Allocated Size(B)	Allocated memory size (byte)
Alloc Cnt	Memory allocation count
Free Cnt	Memory releasing count
Runtime(ms)	Runtime (millisecond)
5Sec	Percentage of cpu resources occupied by the resource user in 5 seconds
1Min	Percentage of cpu resources occupied by the resource user in 1 minute
5Min	Percentage of cpu resources occupied by the resource user in 5 minutes

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show resource policy

Display SRM monitoring policy.

show resource policy { **all** | *policy-name* } [**slot** *slot-id* [**subsystem** *subsystem-id*]]

Parameter Description

Parameter	Description
all	All policies.
policy-name	Name of specific policy.
slot *slot-id*	Specify the board card to be displayed.
subsystem *subsystem-id*	Subsystem id (range: 0-1), equivalent to the cpu id displayed after executing the **show version** command.

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

Example 1: Display all SRM policy information.

```
Ruijie#show resource policy all
policy Name: rgnos_global_policy
----------------------------------------------------------------
Type: Global
In Use: No
RO memory:
critical rising 98 interval 2600 falling 40 interval 2600
major rising 80 interval 4000 falling 30 interval 4000
minor rising 45 interval 6600 falling 10 interval 6600
RO cpu:
critical rising 99 interval 1800 falling 20 interval 1800
major rising 85 interval 3800 falling 40 interval 3800
minor rising 60 interval 6900 falling 10 interval 6900

policy Name: rgnos_policy4
----------------------------------------------------------------
Type: User
In Use: No
RO memory:
critical rising 92 interval 2500 falling 20 interval 2500
major rising 79 interval 3000 falling 40 interval 3000
minor rising 63 interval 5000 falling 10 interval 5000
RO cpu:
```

```
critical rising 89 interval 2900 falling 20 interval 2900
major rising 86 interval 3800 falling 40 interval 3800
minor rising 61 interval 5900 falling 10 interval 5900
Policy Name: rgnos_policy3
----------------------------------------------------------------
Type: User
In Use: No
RO memory:
critical rising 92 interval 2500 falling 20 interval 2500
major rising 79 interval 3000 falling 40 interval 3000
minor rising 63 interval 5000 falling 10 interval 5000
RO cpu:
critical rising 89 interval 2900 falling 20 interval 2900
major rising 86 interval 3800 falling 40 interval 3800
minor rising 61 interval 5900 falling 10 interval 5900
```

Field	Description
Policy Name	Name of monitoring policy
Type	Type of monitoring policy
In Use	In use or not
RO memory	Resource owner - memory
RO cpu	Resource user - cpu

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show resource relationship

Display the association between SRM policy and RU group.

show resource relationship [**slot** *slot-id* [**subsystem** *subsystem-id*]]

Parameter Description

Parameter	Description
slot *slot-id*	Specify the board card to be displayed.
subsystem *subsystem-id*	Subsystem id (range: 0-1), equivalent to the cpu id displayed after executing "show version" command.

Defaults

N/A

Command

Global configuration mode.

Mode

Usage Guide N/A

Configuration Examples

Example 1: Display all SRM association information

```
Ruijie#show resource relationship
Policy                 Resource User       User Type
---------------------------------------------------------------
global                 global              Global Group
rgnos_policy1          rgnos_group     Multi-User Group
rgnos_policy           ktimer              Single-User Group
```

Field	Description
Policy	Monitoring policy
Resource User	Resource user (group)
User Type	Group type, including Global Group, Multi-User Group and Single-User Group with the meaning of global group, multi-user group and single-user group respectively.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show resource user

Display RU configurations.

show resource user { **all** | **group** { **all** | *group-name*} | *resource-user-name* } [**slot** *slot-id* [**subsystem** *subsystem-id*]]

Parameter Description

Parameter	Description
all	All resource users.
group { **all** | *group-name*}	group: Resource user group; all: All resource user groups; *group-name*: Name of resource user group.
resource-user-name	Name of resource user.
slot *slot-id*	Specify the board card to be displayed.
subsystem *subsystem-id*	Subsystem id (range: 0-1), equivalent to the cpu id displayed after executing the **show version** command.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples Example 1: Display all RU group information.

```
Ruijie#show resource user all
Total resource user group: 2.
Multi-User Group: rgnos_group
----------------------------------------------------------
       Policy: rgnos_policy1
       User:
       Resource Owner: memory
              Allocated Size(B): 0
              Alloc Cnt:    0
              Free Cnt: 0
       Resource Owner: cpu
       Runtime(ms)  5Sec        1Min        5Min
       3661500        0         0           0

Single-User Group: ktimer
----------------------------------------------------------
       Policy:      rgnos_policy
       User:        ktimer
       Resource Owner: memory
              Allocated Size(B): 0
              Alloc Cnt:    0
              Free Cnt: 0
       Resource Owner: cpu
       Runtime(ms)      5Sec        1Min        5Min
       3685640              0           0           0
```

Field	Description
Multi-User Group	Multi-user resource user group
Single-User Group	Single-user resource user group
Policy	Monitoring policy
User	Resource user
Resource Owner	Resource owner
Allocated Size(B)	Allocated memory size (byte)
Alloc Cnt	Memory allocation count
Free Cnt	Memory releasing count
Runtime(ms)	Runtime (millisecond)
5Sec	Percentage of cpu resources occupied by the resource user in 5 seconds

1Min	Percentage of cpu resources occupied by the resource user in 1 minute
5Min	Percentage of cpu resources occupied by the resource user in 5 minutes

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

user

In the srm configuration mode, use this command to apply the monitoring policy to a resource user.

user *resource-user-name resource-policy-name*

no user *resource-user-name*

Parameter Description

Parameter	**Description**
resource-user-name	Name of resource user. Execute the **show resource database** command to display the information about resource users.
resource-policy-name	Name of monitor policy.
no	Remove the association between resource user and monitoring policy.

Defaults

N/A

Command Mode

srm configuration mode.

Usage Guide

N/A

Configuration Examples

Example 1: Configure a user monitoring policy named rgos_policy and apply to snmpd.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user snmpd rgos_policy
```

Related Commands

Command	**Description**
resource manager	Enter the SRM configuration mode.

policy policy-*name*	Create the monitoring policy and enter the SRM-policy configuration mode.

Platform Description

N/A

user global

In the srm configuration mode, use this command to apply the monitoring policy to the global resource user group.

user global *global-policy-name*

no user global

Parameter Description

Parameter	Description
global-policy-name	Name of global monitoring policy.
no	Remove the association between group resource user and monitoring policy.

Defaults

N/A

Command Mode

srm configuration mode

Usage Guide

N/A

Configuration Examples

Example 1: Configure a global monitoring policy named rgos_policy and apply to the global resource user group.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#policy rgos_policy global
Ruijie(config-srm-policy)#exit
Ruijie(config-srm)#user global rgos_policy
```

Related Commands

Command	Description
resource manager	Enter the SRM configuration mode.
policy policy-*name*	Create the monitoring policy and enter the SRM-policy configuration mode.

Platform Description

N/A

user group

In the srm configuration mode, use this command to create the resource user group and enter the config-res-group configuration mode.

user group *resource-group-name*

no user group *resource-group-name*

Parameter Description

Parameter	**Description**
resource-group-name	Name of resource user group.
no	Remove the resource user group.

Defaults

N/A

Command Mode

SRM configuration mode.

Usage Guide

N/A

Configuration Examples

Example 1: Configure a resource user group named rgos_group.

```
Ruijie#configure terminal
Ruijie(config)#resource manager
Ruijie(config-srm)#user group rgos_group
Router(config-res-group)#
```

Related Commands

Command	**Description**
resource manager	Enter the SRM configuration mode.

Platform Description

N/A

Hardware Entry Capacity Commands

initialization route unicast

Use this command to configure the maximum number of unicast routes.

initialization route unicast *max_num*

no initialization route unicast

Parameter Description

Parameter	Description
max_num	The maximum number of unicast routes.

Defaults 130 unicast routes.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of unicast routes to 260:

```
Ruijie(config)# initialization route unicast ?
  <1-260>  Max capacity of unicast route entry
Ruijie(config)# initialization route unicast 260
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A.

initialization route shared-pool

Use this command to configure the maximum number of the shared pools.

initialization route shared-pool *max_num*

no initialization route shared-pool

Parameter Description

Parameter	Description
max_num	The maximum number of the shared pools, which are shared by MPLS,vlan-mapping, mac-vlan, subnet-vlan and qinq-adv functions.

Defaults

1024 shared pool entries.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example configures the maximum number of the shared pools to 1000:

```
Ruijie(config)# initialization route tunnel-termination ?
  <0-1024>  max capacity of mpls/vlan-mapping/mac-vlan/subnet-vlan/qinq-adv
entry
Ruijie(config)# initialization route tunnel-termination 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A.

show initialization route

Use this command to show the hardware entry capacity.

show initialization route

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to show the configuration value, the current running value and the default value of all types of hardware entry capacities.

Configuration Examples

The following example displays the hardware entry capacity:

```
Ruijie #show initialization route


                             config  running  default
 policy-based route entry:   64      64       64
 tunnel termination entry:   32      32       32
```

```
shared-pool entry:        200    200     200
```

Field	Description
config	Indicates the current configuration which is invalid.
running	Indicates the current running status which has taken effect.
default	Indicates the system default value.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Ethernet Switching Configuration Commands

1. Interface Configuration Commands
2. MAC Address Configuration Commands
3. Aggregate Port Configuration Commands
4. LACP Configuration Commands
5. VLAN Configuration Commands
6. Protocol VLAN Configuration Commands
7. Private VLAN Configuration Commands
8. Share VLAN Configuration Commands
9. Voice VLAN Configuration Commands
10. MAC VLAN Configuration Commands
11. MSTP Configuration Commands
12. Protocol Frames Transparent Transmission Configuration Commands
13. GVRP Configuration Commands
14. LLDP Configuration Commands
15. QinQ Configuration Commands
16. ERPS Configuration Commands

Interface Configuration Commands

carrier-delay

In interface configuration mode, use the **carrier-delay** command to set the carrier delay on the interface, and the no carrier-delay command to restore it to default.

carrier-delay [*seconds*]

no carrier-delay

Parameter Description

Parameter	Description
seconds	Optional parameter within the range of 1 to 60 seconds

Defaults

The default carrier delay is 2 seconds.

Command Mode

Interface configuration mode

Usage Guide

This parameter refers to the delay after which the carrier detection signals DCD of the interface link turns from the Down status to the Up status. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation.

If the DCD carrier is disconnected for a long time, the parameter should be increased to accelerate route aggregation and routing table convergence. If the DCD carrier interruption period is shorter than the time used for route aggregation, you should raise the parameter to avoid unnecessary route oscillation.

Configuration Examples

The following example shows how to configure the carrier delay of serial interface as 5 seconds:

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config)# carrier-delay 5
```

Related Commands

Command	Description
-	-

Platform Description

N/A

clear counters

Use this command to clear the counters on a specified interface.

clear counters [*interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface type and interface ID

Defaults

Command Mode Privileged EXEC mode.

Usage Guide In the privileged EXEC mode, use the **show interfaces** command to display counters or the **clear counters** command to clear counters. If no interface is specified, the counters on all interfaces will be cleared.

Configuration Examples

```
Ruijie# clear counters gigabitethernet 1/1
```

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description N/A

clear interface

Reset the interface hardware.

clear interface *interface-id*

Parameter Description

Parameter	Description
interface-id	Interface type and interface ID

Defaults

Command Mode Privileged EXEC mode.

Usage Guide This command is only used on the switch port, member port of the L2 Aggregate port and routing port. This command is equivalent to the **shutdown** and **no shutdown** commands.

Configuration Examples

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

Related Commands

Command	Description
shutdown	Shutdown the interface.

Platform Description

N/A

description

Use this command to set an interface alias. Add **no** in the command to restore the defaults.

description *string*

no description

Parameter Description

Parameter	Description
string	Interface alias

Defaults

By default, there is no alias.

Command Mode

Interface configuration mode.

Usage Guide

Use the **show interfaces** command to display the interface information, including the alias.

Configuration Examples

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

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

duplex

Use the **duplex** command in the interface configuration mode to specify the duplex mode for the interface. Add **no** in the command to restore it to the default.

duplex {auto | full | half}

no duplex

Parameter Description

Parameter	Description
auto	Self-adaptive full duplex and half duplex
full	Full duplex
half	Half duplex

Defaults

Auto.

Command Mode

Interface configuration mode.

Usage Guide

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

Configuration Examples

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

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

flowcontrol

Use this command to enable or disable the flow control. Add **no** in the command to restore it to the default setting.

flowcontrol {auto | off | on | receive {auto | off | on } | send {auto | off | on}}

no flowcontrol

Parameter Description

Parameter	Description
auto	Self-negotiate the flow control.
off	Disable the flow control.
on	Enable the flow control.
receive	Receiving direction of the non-symmetric flow control.
send	Sending direction of the non-symmetric flow control.

Defaults

By default, flow control is disabled.

Command Mode

Interface configuration mode.

Usage Guide

Use the **show interfaces** command to display the flow control configurations.

Configuration Examples

This example shows how to enable flow control on fastEthernet port 1/1:

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

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

interface aggregateport

Use this command to access or create an aggregate port and enter the interface configuration mode. Add **no** in the command to remove this port.

interface aggregateport *port-number*

Parameter Description

Parameter	Description
port-number	Aggregate port number. Its range varies with the equipment and extended modules.

Defaults

Command Mode

Global configuration mode.

Usage Guide

Based on certain rules, you can add other ports to an aggregate port. All the members of an aggregate port are considered as a whole, and their attributes vary with the ones of the aggregate port. You can use **show interfaces** or **show interfaces aggregateport** commands to display the interface configuration.

Configuration Examples

```
Ruijie(config)#interface aggregateport 3
Ruijie(config-if)#
```

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

1. Up to 8 member ports can be configured.
2. Up to 120 aggregation ports can be configured globally.

interface fastEthernet

Use this command to select an Ethernet interface, and enter the interface configuration mode.

interface fastEthernet *mod-num/port-num*

Parameter Description

Parameter	Description
mod-num/port-num	The range varies with the device and the extended module.

Defaults

Command Mode Global configuration mode.

Usage Guide The command does not support the **no** parameter, so this interface type cannot be deleted. Use **show interfaces** or **show interfaces fastEthernet** to display the interface configuration.

Configuration Examples

```
Ruijie(config)# interface fastEthernet 1/2
Ruijie(config-if)#
```

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description N/A

interface giagbitEthernet

Use this command to select a Gigabit Ethernet interface, and enter the interface configuration mode.

interface gigabitEthernet *mod-num/port-num*

Parameter Description

Parameter	Description
mod-num/port-num	The range varies with the device and the extended module.

Defaults

Command Mode Global configuration mode.

Usage Guide

The command does not support the **no** parameter, so this interface type cannot be deleted. Use **show interfaces** or **show interfaces gigabitEthernet** to display the interface configuration.

Configuration Examples

```
Ruijie(config)# interface gigabitEthernet 1/2
Ruijie(config-if)#
```

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

interface vlan

Use the interface vlan command in the global configuration mode to access or create the SVI (Switch Virtual Interface). Add **no** in the command to remove the SVI.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Parameter Description

Parameter	Description
vlan-id	VLAN ID. Its range depends by products.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

Use **show interfaces** or **show interfaces vlan** to display the interface configuration.

Configuration Examples

```
Ruijie(config)# interface vlan 2
Ruijie(config-if)#
```

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

line-detect

Use this command to detect the cable connection status.

line-detect

Parameter Description

Parameter	Description

Defaults

Command Mode

Interface configuration mode.

Usage Guide

This command is used to show the line status and locate the cause of a line failure; for example, the line is broken.

Configuration Examples

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#line-detect

Interface : GigabitEthernet 0/1
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state     length(meters)
---- ---------- --------------
A    Ok        1
pair state     length(meters)
---- ---------- --------------
B    Ok        2
pair state     length(meters)
---- ---------- --------------
C    Short     1
pair state     length(meters)
---- ---------- --------------
D    Short     1
```

Field	Description

pairs	The number of line pairs included. For example, the twisted pair comprises four pairs of lines.
state	Status of the current line pair: **OK**, **Short** or **Open**. In general, the 100 Mbit/s twisted pairs A and B are OK, C and D are Short. The 1000 Mbit/s twisted pairs A, B, C and D are all OK.
length	Length of the line in meter. Only the length of the OK line pair is effective. Because the length is calculated based on the signal transmission time, there may be a certain difference. The length of a Short or Open line pair measures the distance from the port to the faulty point.

Related Commands

Command	Description

Platform Description

N/A

medium-type

Use this command to select the medium type for an interface. Add **no** in the command to restore it to the default setting.

medium-type { auto-select [prefer [fiber | copper]] | fiber | copper }

Parameter Description

Parameter	Description
fiber	Optical interface.
prefer[fiber| copper]	The preferred medium type for the interface is selected.
auto-select	Auto-select the medium type for the interface.
copper	Copper interface.

Defaults

Copper interface.

Command Mode

Interface configuration (physical interface, except for AP and SVI)

Usage Guide

If a port can be used as an optical or electrical port, you can only select either. Once the media type is specified, the attributes of the port such as status, duplex, flow control, and rate, apply to the currently selected media type. After the port type is changed, the attributes of the new port type take default values, which can be modified as needed.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# medium-type copeer
```

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

mtu

Use this command to set the MTU on the interface.

mtu *num*

Parameter Description

Parameter	Description
num	64 to 9,216 (or 65,536, which varies by products)

Defaults

By default, the num is 1,500.

Command Mode

Interface configuration mode.

Usage Guide

Set the maximum transmission unit (MTU) that is supported on the interface.

Configuration Examples

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

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

shutdown

Use the **shutdown** command in the interface configuration mode to disable an interface. Add **no** in the command to enable a disabled port.

shutdown

no shutdown

Parameter Description

Parameter	Description

Defaults

Command Mode

Interface configuration mode

Usage Guide

Use this command to stop forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port to support the **no shutdown** command. If you shut down the interface, the configuration of the interface does not take effect. You can view the interface status by using the **show interfaces** command.

> ⚠ Caution If you use the script to run **no shutdown** frequently, the system may display the interface status reversal.

Configuration Examples

```
Shut down Ap 1:
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# shutdown
Enable Ap 1:
Ruijie(config)# interface aggregateport 1
Ruijie(config-if)# no shutdown
```

Related Commands

Command	Description
clear interface	Reset the hardware.
show interfaces	Show the interface information.

Platform Description

N/A

snmp trap link-status

You can set up whether to send LinkTrap on an interface. If the function is enabled, the SNMP will send the LinkTrap when the link status of the interface changes. The **no** attribute of this command prevents the SNMP from sending the LinkTrap.

snmp trap link-status

no snmp trap link-status

Parameter Description

Parameter	Description

Defaults

This function is enabled. If the link status of the port changes, the SNMP sends the LinkTrap.

Command Mode

Interface configuration mode.

Usage Guide

For an interface such as Ethernet interface, AP interface, and SVI interface, this command determines whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

Configuration Examples

Do not send LinkTrap on the interface:

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

Following configuration shows how to configure the interface to forwarding Link trap:

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# snmp trap link-status
```

Related Commands

Command	Function
Ruijie(config-if)# snmp trap link-status	Enable sending LinkTrap on the interface.
Ruijie(config-if)# no snmp trap link-status	Disable sending LinkTrap on the interface.

Platform Description

N/A

speed

Use this command to configure the transmission speed on the interface. Use the **no** form of this command to restore the default setting.

speed [**10 | 100 | 1000 | 10G | auto**]

no speed

Parameter Description

Parameter	Description
10	The transmission rate of the interface is 10 Mbps.
100	The transmission rate of the interface is 100 Mbps.
1000	The transmission rate of the interface is 1000 Mbps.
10G	The transmission rate of the interface is 10 Gbps.
auto	The transmission rate of the interface is adaptive.

Defaults

Auto.

Command Mode

Interface configuration mode.

Usage Guide

If an interface is an aggregate port member, its rate may vary with that of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use the **show interfaces** command to display the configuration. The rate allowed to be set varies with the interface type. For example, you cannot set the rate of an SFP interface to 10 Mbps.

Configuration Examples

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

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

switchport

In the interface configuration mode, you can use **switchport** without any parameter to configure an interface to work in Layer 2 mode. Use the **no switchport** command without any parameter to configure it as Layer 3 interface.

switchport

no switchport

Parameter Description

Parameter	Description
N/A	N/A

Defaults

All the interfaces work in Layer 2 mode by default.

Command Mode

Interface configuration mode.

Usage Guide

This command applies only to physical interfaces. The **switchport** command is used to disable and re-enable an interface. In this status, the device will send the information to indicate the connect status. If the interface switches from Layer 2 to Layer 3 mode, all the attributes in Layer 2 mode will be cleared.

Configuration Examples

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

Related Commands

Command	Description
show interfaces	Show the interface information.

Platform Description

N/A

switchport access

Use this command to configure an interface as an access port and assign it to a VLAN. Add **no** in 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 for a port to be added.

Defaults

By default, the switch port is an access port and the VLAN is VLAN 1.

Command Mode

Interface configuration mode.

Usage Guide

Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN.

If the port is a trunk port, the operation does not take effect.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	Set up the interface to work in Layer 2 mode (switch port mode).
switchport trunk	Use this command to specify a native VLAN and the allowed-VLAN list for the trunkport.

Platform Description

N/A

switchport mode

Use this command to assign a L2 interface (switch port) mode. You can designate this interface as an access port or a trunk port or an 802.1Q tunnel. Add **no** in the command to restore it to the default.

switchport mode {access | trunk}

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.

Defaults

By default, the switch port is an access port.

Command Mode

Interface configuration mode.

Usage Guide

If a switch port is an access port, it can be a member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN.

A trunk port can be a member port of various VLANs on the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs of the interface. The trunk port is the member of all the VLANs on the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.

Configuration Examples

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

Related Commands

Command	Description
switchport access	Use this command to configure an interface as a static 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 trunk port.

Platform Description

N/A

switchport trunk

Use this command to assign a native VLAN and the allowed-VLAN list for the trunk port. Add **no** in the command to restore it to 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 that are separated by hyphens; for example, 10 to 20. The segments can be separated by a comma (,), for example, 1 to 10, 20 to 25, 30, and 33. all: The allowed VLAN list contains all supported VLANs; add: adds a specified VLAN list to the allowed VLAN list; remove: removes a specified VLAN list from the allowed VLAN list; except: adds all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
native vlan *vlan-id*	Specify the native VLAN.

Defaults

The allowed VLAN list is all, the Native VLAN is VLAN1.

Command Mode

Interface configuration mode.

Usage Guide

Native VLAN:

A Trunk port belongs to one native VLAN. Untagged packets that are received or 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 within the native VLAN are sent over the trunk port, they are untagged.

Allowed-VLAN List:

By default, a trunk port receives and sends traffic from or to all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing through the trunk by configuring allowed VLAN lists.

Use show interfaces switchport to display configuration.

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
Switchport is enabled
Mode is trunk port
Access vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is
1,3-4094
```

Related Commands

Command	Description
show interfaces	Show the interface information.
switchport access	Use this command to configure an interface as a static access port and assign it to a VLAN.

Platform Description

N/A

show interfaces

Use this command to show the interface information, statistical information and optical module information.

show interfaces [*interface-id*] [**counters** [**module** *module-id* | **nonzero** | **vlan** *vlan-id*] | **description** | **mtu** | **status** [**module** *module-id* | **vlan** *vlan-id*] | **switchport** | **trunk** | **transceiver** [**alarm** | **diagnosis**] | **usage**]

Parameter Description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregate port, SVI interface, loopback interface and VSL interface).
counters	The statistics on the interface.
counters module *module-id*	Display the packet statistics of all ports on the specified modules.
counters nonzero	Display the interface (including Ethernet interface, aggregate port and VSL interface) statistics information (0 excluded).
counters vlan *vlan-id*	Display the packet statistics of all member ports in the specified vlans.
description	Describes the interface, including its link status.
mtu	Display the MTU statistics of the ports (including Ethernet interfaces and aggregate ports)
status	Display the status of all the link of the Layer 2 interface, including the rate and duplex.
status module	Display the status statistics of all member ports on the

module-id	specified modules.
status vlan *vlan-id*	Display the status statistics of all member ports in the specified vlans.
switchport	Information about Layer 2 interface.
trunk	Trunk port, which applies to physical and aggregate ports.
transceiver	Basic optical module information.
transceiver alarm	Alarm information of the optical module. “None” is displayed when no fault occurs.
transceiver diagnosis	Diagnosis parameter value of the optical module.
line-detect	Line detecting status of the port.
usage	Display the bandwidth usage rate on the interface (including Ethernet interfaces and aggregate ports).

Defaults

Show all the information.

Command Mode

Privileged EXEC mode.

Usage Guide

Show the basic information if no parameter is specified.

The functions of showing the optical module information, raising fault alarms and diagnosing parameters must be used together with the optical modules of the RG network.

To show the optical module information and give fault alarms and diagnose parameters, the optical module must support Digital Diagnostic Monitoring.

Configuration Examples

Example 1 shows the interface information when the Gi0/1 is a Trunk port:

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
flow receive control admin status is OFF,flow send control admin
status is OFF,flow receive control oper status is Unknown,flow
send control oper status is Unknown
broadcast  Storm  Control  is  OFF,multicast  Storm  Control  is
OFF,unicast Storm Control is OFF
 Port-type: trunk
   Native vlan:1
Allowed vlan lists:1-4094
Active vlan lists:1, 3-4
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Example 2 shows the interface information when the Gi0/1 is an Access port:

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
flow receive control admin status is OFF,flow send control admin
status is OFF,flow receive control oper status is Unknown,flow
send control oper status is Unknown
broadcast  Storm  Control  is  OFF,multicast  Storm  Control  is
OFF,unicast Storm Control is OFF
```

```
Port-type: access
Vlan id : 2
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Example 3 shows information about the layer-2 interface when the Gi0/1 is a Hybrid port.

```
SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
flow receive control admin status is OFF,flow send control admin
status is OFF,flow receive control oper status is Unknown,flow
send control oper status is Unknown
broadcast  Storm  Control  is  OFF,multicast  Storm  Control  is
OFF,unicast Storm Control is OFF
Port-type: hybrid
Tagged vlan id:2
Untagged vlan id:none
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
```

```
   0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

Example 4 shows the layer-2 information of the Gi0/1 port.

```
Ruijie# show interfacesgigabitEthernet 0/1 switchport
Interface Switchport ModeAccess Native Protected VLAN lists
--------- ---------- --------- ------ ------ ---------
GigabitEthernet 0/1 enabled Access 11  Disabled  ALL
```

Example 5 shows the optical module information the Gi0/1 port.

```
Ruijie# show interfaces gigabitEthernet 0/1 transceiver
Transceiver Type    :  1000BASE-SX-SFP
Connector Type     :  LC
Wavelength(nm)     :  850
Transfer Distance   :
   50/125 um OM2 fiber
      -- 550m
   62.5/125 um OM1 fiber
      -- 270m
Digital Diagnostic Monitoring  : YES
Vendor Serial Number         : 101680093602489
```

Example 6 shows the current measured value of the optical module diagnosis parameter on the Gi0/1 port.

```
Ruijie#  show  interfaces  gigabitEthernet  0/1  transceiver
diagnosis
Current diagnostic parameters[AP:Average Power]:
Temp(Celsius)    Voltage(V)        Bias(mA)                RX
power(dBm)      TX power(dBm)
38(OK)                      3.20(OK)                 0.04(OK)
-40.00(alarm)[AP]   -40.00(alarm)
```

Example 7 shows the current failure warning information of the optical module on the Gi0/1port.

```
Ruijie# show interfaces gigabitEthernet 0/1 transceiver alarm
RX power low
TX power low
```

Example 8 shows the packet statistics (0 excluded) information on ports (only displays the information of parts of the ports, not the information of all ports)

```
Ruijie# show interfaces counters nonzero
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets           : 408
```

```
InUcastPkts         : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets           : 408
OutUcastPkts        : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions          : 0
Fragments           : 0
Jabbers             : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors           : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets            : 408
InUcastPkts         : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets           : 408
OutUcastPkts        : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions          : 0
Fragments           : 0
Jabbers             : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors           : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

Example 9 shows the packet statistics of the ports on Module 1/0 (only displays the information of parts of the ports, not the information of all ports).

```
Ruijie# show interfaces counters module 1/0
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets           : 408
InUcastPkts         : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets          : 408
OutUcastPkts        : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions          : 0
Fragments          : 0
Jabbers            : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors          : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets           : 408
InUcastPkts         : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets          : 408
```

```
OutUcastPkts       : 4
OutMulticastPkts    : 0
OutBroadcastPkts    : 0
Undersize packets   : 0
Oversize packets    : 0
collisions         : 0
Fragments          : 0
Jabbers           : 0
CRC alignment errors : 0
AlignmentErrors     : 0
FCSErrors          : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

Example 10 shows the packet statistics of all member ports on VLAN 1 (only shows the information of parts of the ports, not the information of all ports).

```
Ruijie# show interfaces counters vlan 1
Interface : GigabitEthernet 1/0/1
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets           : 408
InUcastPkts        : 4
InMulticastPkts     : 0
InBroadcastPkts     : 0
OutOctets          : 408
OutUcastPkts       : 4
OutMulticastPkts    : 0
OutBroadcastPkts    : 0
Undersize packets   : 0
Oversize packets    : 0
collisions         : 0
Fragments          : 0
Jabbers           : 0
CRC alignment errors : 0
AlignmentErrors     : 0
FCSErrors          : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0

Interface : GigabitEthernet 1/0/2
5 minutes input rate  :0 bits/sec, 0 packets/sec
5 minutes output rate :0 bits/sec, 0 packets/sec
InOctets           : 408
InUcastPkts         : 4
InMulticastPkts      : 0
InBroadcastPkts      : 0
OutOctets           : 408
OutUcastPkts        : 4
OutMulticastPkts     : 0
OutBroadcastPkts     : 0
Undersize packets    : 0
Oversize packets     : 0
collisions          : 0
Fragments           : 0
Jabbers            : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors           : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64 : 0
  65-127 : 4
  128-255 : 0
  256-511 : 0
  512-1023 : 0
  1024-1518 : 0
```

Example 11 shows the MTU statistics of the specified GigabitEthernet 0/1 port.

```
Ruijie# show interfaces gigabitethernet 0/1 mtu
Interface                    MTU
-------------------------------- ------
GigabitEthernet 0/1            1500
```

Example 12 shows the status statistics of all ports on Module1/0 (only displays the information of parts of the ports, not the information of all ports).

```
Ruijie# show interfaces status module 1/0
Interface                     Status     Vlan   Duplex    Speed
Type
--------------------------------  --------    ----    -------
--------- ------
GigabitEthernet 1/0/18       down      1     Unknown  Unknown
```

```
copper
GigabitEthernet 1/0/21     down     1    Unknown  Unknown copper
GigabitEthernet  1/0/22      down       1     Unknown   Unknown
copper
GigabitEthernet 1/0/23    down      1    Unknown  Unknown copper
GigabitEthernet 1/0/24    down      1    Unknown  Unknown copper
GigabitEthernet 1/0/25   down      1     Unknown  Unknown copper
```

Example 13 shows the status statistics of all member ports in VLAN 1 (only displays the information of parts of the ports, not the information of all ports).

```
Ruijie# show interfaces status vlan 1
Interface                        Status     Vlan   Duplex    Speed
Type
--------------------------------  --------    ----    -------
--------- ------
GigabitEthernet 1/0/18      down     1    Unknown Unknown copper
GigabitEthernet 1/0/21     down      1     Unknown Unknown copper
GigabitEthernet 1/0/22     down      1     Unknown Unknown copper
GigabitEthernet  1/0/23     down        1      Unknown  Unknown
copper
GigabitEthernet 1/0/24   down      1     Unknown  Unknown copper
GigabitEthernet 1/0/25   down      1     Unknown  Unknown copper
```

Example 14 shows the bandwidth usage value of the specified GigabitEthernet 0/1 port.

```
Ruijie# show interfaces gigabitethernet 0/1 usage
Interface                       Bandwidth    Bandwidth Usage
--------------------------------               -------------
-----------------
GigabitEthernet 0/1            100000   Kbit 0.0%
```

Related Commands

Command	**Description**
duplex	Duplex
flowcontrol	Flow control status.
interface gigabitEthernet	Selects the interface and enter the interface configuration mode.
interface aggregateport	Creates or accesses the aggregate port, and enters the interface configuration mode.
interface vlan	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
shutdown	Disables the interface.
speed	Configures the speed on the port.
switchport priority	Configures the default 802.1q interface priority.
switchport protected	Specifies the interface as a protected port.

Platform Description	N/A

MAC Address Configuration Commands

address-bind

Use this command to configure IP address-MAC address binding. If the **no** form is used, the IP address is unbound from the MAC address.

address-bind *ip-address mac-address*

no address-bind *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address to be bound
mac-address	MAC address to be bound

Defaults N/A

Command Mode Global configuration mode.

Usage Guide If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

Configuration Examples This is an example of binding the IP address 3.3.3.3 and the MAC address 00d0.f811.1112.

```
Ruijie config) # address-bind 3.3.3.3 00d0.f811.1112
```

Related Commands

Command	Description
show address-bind	Show the IP address-MAC address binding table.

Platform Description N/A

address-bind install

This command is used to install a binding policy. If the **no** form is used, the binding policy is uninstalled.

address

no address

Parameter Description

Parameter	Description
-	-

Defaults N/A

Command Mode Global configuration mode.

Usage Guide If you bind an IP address to a MAC address, run this command to make the installation policy take effect.

Configuration Examples Install a binding policy.

```
Ruijie(config)# address-bind 3.3.3.3 00d0.f811.1112
Ruijie(config)# address-bind install
```

Related Commands

Command	Description
-	-

Platform Description N/A

address-bind ip-address

This command is used to bind an IP address to a MAC address. if the **no** form is used, the IP address is unbound from the MAC address.

address-bind *ip-address mac-address*

no address-bind *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address to be bound
mac-address	MAC address to be bound

Defaults N/A

Command mode Global configuration mode.

Usage Guide If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

Configuration Examples This is an example of binding the IP address 3.3.3.3 and MAC address 00d0.f811.1112.

```
Ruijie(config)# address-bind 3.3.3.3 00d0.f811.1112
```

Related Commands

Command	Description
show address-bind	Show the IP address-MAC address binding table.

Platform N/A

Description

address-bind ipv6-mode

This command is used to set the IP mode of IP address binding. If the **no** form is used, the IP mode is canceled.

This command is also used to set the compatible mode.

address-bind ipv6-mode compatible

Set the loose mode.

address-bind ipv6-mode loose

Set the strict mode.

address-bind ipv6-mode strict

no address-bind ipv6-mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults Strict mode

Command Mode Global configuration mode.

Usage Guide There are three IP address binding modes: compatible, loose and strict. The following table shows the forwarding rules corresponding to binding modes.

Mode	IPv4 forwarding rule
Strict	Only the packets matching IPv4 and MAC are forwarded.
Loose	Only the packets matching IPv4 and MAC are forwarded.
compatible	Only the packets matching IPv4 and MAC are forwarded.

Mode	IPv6 forwarding rule
Strict	No IPv6 packets can be forwarded. (default mode)
Loose	All IPv6 packets can be forwarded.
compatible	Only the IPv6 packets with the source MAC address being bound MAC address.

Configuration Examples

Bind the IP address 192.168.5.2 and the MAC address 00do.f822.33aa and forward the corresponding packets:

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.2 00d0.f822.33aa
Ruijie(config)# address-bind ipv6-mode compatible
```

Related Commands

Command	Description
show address-bind uplink	Show the exceptional port of the address binding.

Platform Description

N/A

address-bind uplink

This command is used to configure the exception port policy.

address-bind uplink *intf-id*

no address-bind uplink *intf-id*

Parameter Description

Parameter	Description
intf-id	Exceptional port

Defaults

-

Command Mode

Global configuration mode.

Usage Guide

If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

Configuration Examples

Following example is to set the fa 0/1 port as an exceptional port for address binding.

```
Ruijie(config)#address-bind uplink fa0/1
```

Related Commands

Command	Description
show address-bind uplink	Show the exceptional port of address binding.

Platform Description

N/A

clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

clear mac-address-table dynamic [**address** *mac-addr* [**interface** *interface-id*] [**vlan** *vlan-id*]

Parameter Description

Parameter	Description
dynamic	Clear all the dynamic MAC addresses.
address *mac-addr*	Clear the specified dynamic MAC address.
interface *interface-id*	Clear all the dynamic MAC addresses of the specified interface.
vlan *vlan-id*	Clear all the dynamic MAC addresses of the specified VLAN.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use **show mac-address-table dynamic** to display all the dynamic MAC addresses.

Configuration Examples Clear all the dynamic MAC addresses:

```
Ruijie# clear mac-address-table dynamic
```

Related Commands

Command	Description
show mac-address-table dynamic	Use this command to display dynamic MAC address.

Platform Description N/A

mac-address-learning

This command is used to enable the port address learning. If the **no** option is used, the port address learning function is disabled.

mac-address-learning

no mac-address-learning

Parameter Description

Parameter	Description
-	-

Defaults The address learning function is enabled.

Command Mode Interface mode.

Usage Guide MAC address learning cannot be disabled on the port where the security function is enabled. The security function cannot be configured on the port where address learning is disabled.

Configuration Examples Disable the port address learning function.

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

Related Commands

Command	Description
-	-

Platform Description

N/A

mac-address-table aging-time

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

mac-address-table aging-time *seconds*

no mac-address-table aging-time

Parameter Description

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

Defaults

300 seconds.

Command Mode

Global configuration mode.

Usage Guide

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

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

Configuration Examples

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

Related Commands

Command	Description
show mac-address-table aging-time	Use this command to display the aging time of the dynamic MAC address.
show mac-address-table dynamic	Use this command to display dynamic MAC address.

Platform Description

N/A

mac-address-table filtering

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

mac-address-table filtering *mac-address* **vlan** *vlan-id* [source | destination]

no mac-address-table filtering *mac-address* **vlan** *vlan-id*

Parameter Description

Parameter	Description
mac-address	Filtering Address
vlan *vlan-id*	VLAN ID. Its range depends on the switch.
source	Filter the frame according to the source MAC address only.
destination	Filter the frame according to the destination MAC address only.

Defaults

No filtering address is configured by default.

When configuring this command without the **source** or **destination** specified, the frame received in the specified VLAN, which has the same source/destination MAC address with the specified MAC address, will be filtered.

Command Mode

Global configuration mode.

Usage Guide

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

Configuration Examples

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

Related Commands

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

Platform Description

N/A

mac-address-table notification

Use this command to enable the MAC address notification function. You can use The **no** form of the command to disable this function.

mac-address-table notification [**interval** *value* | **history-size** *value*]

no mac-address-table notification [**interval** | **history-size**]

Parameter Description

Parameter	Description
interval *value*	Specify the interval of sending the MAC address trap message, 1 second by default.
history-size *value*	Specify the maximum number of the entries in the MAC address notification table, 50 entries by default.

Defaults

By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.

Command Mode

Global configuration mode.

Usage Guide

The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the **snmp-server enable traps mac-notification** command to enable or disable the switch to send the MAC address trap message.

Configuration Examples

```
Ruijie(config)# mac-address-table notification
Ruijie(config)# mac-address-table notification interval 40
Ruijie(config)# mac-address-table notification history-size 100
```

Related Commands

Command	Description
snmp-server enable traps	Set the method of handling the MAC address trap message..
show mac-address-table notification	Show the MAC address notification configuration and the MAC address trap notification table.
snmp trap mac-notification	Enable the MAC address trap notification function on the specified interface.

Platform Description

N/A

mac-address-table static

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

mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Parameter Description

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

Defaults

No static MAC address is configured by default.

Command Mode

Global configuration mode.

Usage Guide

A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use show mac-address-table static to display the static MAC address.

Configuration

When the packet destined to 00d0 f800 073c arrives at VLAN4, it will be forwarded to the specified

Examples

port gigabitethernet 1/1:

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

Related Commands

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

Platform Description

N/A

show address-bind

Use this command to show IP address-MAC address binding.

show address-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie# show address-bind
IP Address   Binding MAC Addr
------------  -----------------
3.3.3.3    00d0.f811.1112
3.3.3.4    00d0.f811.1117
```

Related Commands

Command	Description
address-bind	Enable IP address-MAC address binding.

Platform Description

N/A

show address-bind uplink

Use this command to show the exceptional port.

show address-bind uplink

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode N/A

Usage Guide N/A

Configuration Examples

```
Ruijie# show address-bind uplink
Ports    State
------------ ------
Fa0/1    Disabled
Fa0/2    Disabled
......
```

Related Commands

Command	Description
address-bind uplink	Set the exceptional port.

Platform Description N/A

show mac-address-learning

Use this command to show the MAC address learning.

show mac-address-learning

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example shows the MAC address learning

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mac-address-table address

Use this command to show all types of MAC addresses (including dynamic address, static address and filtering address)

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

Parameter Description

Parameter	Description
address *mac-addr*	Specified MAC address.
interface *interface-id*	Interface ID
vlan *vlan-id*	VLAN ID

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mac-address-table address 00d0.f800.1001
Vlan    MAC Address     Type   Interface
---------- -------------------- --------
1     00d0.f800.1001    STATIC  Gi1/1
```

Related Commands

Command	Description
show mac-address-table static	Show the static MAC address.
show mac-address-table filtering	Show the filtering MAC address.
show mac-address-table dynamic	Show the dynamic MAC address.
show mac-address-table interface	Show all types of MAC addresses of the specified interface
show mac-address-table vlan	Show all types of MAC addresses of the specified VLAN
show mac-address-table count	Show the address counts in the MAC address table.
show mac-address-table static	Show the static MAC address.
show mac-address-table filtering	Show the filtering MAC address.

Platform Description N/A

show mac-address-table aging-time

Use this command to display the aging time of the dynamic MAC address.

show mac-address-table aging-time

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide

Configuration Examples

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

Related Commands

Command	Description
mac-address-table aging-time	Specify the aging time of the dynamic MAC address.

Platform Description N/A

show mac-address-table count

This command is used to display the number of address entries in the address table.

show mac-address-table count [interface *interface-id* **| vlan** *vlan-id***]**

Parameter Description

Parameter	Description
interface *interface-id*	Interface ID
vlan *vlan-id*	VLAN ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide The **show mac-address-table count** command is used to display the number of entries based on the type of MAC address entry.

The **show mac-address-table count interface** command is used to display the number of entries based on the interface associated with the MAC address entry.

The **show mac-address-table count vlan** command is used to display the number of entries based on the VLAN of MAC address entries.

Configuration Examples Example 1: Display the number of MAC address entries.

```
Ruijie# show mac-address-table count
Dynamic Address Count : 51
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses  : 51
Total Mac Address Space Available: 8139
```

Example 2: Display the number of MAC address in VLAN 1.

```
Ruijie# show mac-address-table count vlan 1
Dynamic Address Count : 7
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses   : 7
```

Example 3: Display the number of MAC addresses on interface g0/1.

```
Ruijie# show mac-address-table interface g0/1
Dynamic Address Count : 10
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses   : 10
```

Related Commands

Command	Description
show mac-address-table static	Display the static address.
show mac-address-table filtering	Display the filtering address.
show mac-address-table dynamic	Display the dynamic address.
show mac-address-table address	Display all the address information of the specified address.
show mac-address-table interface	Display all the address information of the specified interface.
show mac-address-table vlan	Display all the address information of the specified vlan.

Platform Description

N/A

show mac-address-table dynamic

Use this command to show the dynamic MAC address.

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

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN of the entry
interface-id	Interface that the packet is forwarded to. It may be a physical port or an aggregate port

Defaults

All the MAC addresses are displayed by default.

Command Mode

Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mac-address-table dynamic
Vlan   MAC Address     Type   Interface
------------------------- -------- -------------------
1   0000.0000.0001   DYNAMIC gigabitethernet 1/1
1   0001.960c.a740   DYNAMIC gigabitethernet 1/1
1   0007.95c7.dff9   DYNAMIC gigabitethernet 1/1
1   0007.95cf.eee0   DYNAMIC gigabitethernet 1/1
1   0007.95cf.f41f   DYNAMIC gigabitethernet 1/1
1   0009.b715.d400   DYNAMIC gigabitethernet 1/1
1   0050.bade.63c4   DYNAMIC gigabitethernet 1/1
```

Related Commands

Command	Description
clear mac-address-table dynamic	Clear the dynamic MAC address.

Platform Description N/A

show mac-address-table filtering

Use this command to show the filtering MAC address.

show mac-address-table filtering [**addr** *mac-addr*] [**vlan** *vlan-Id*]

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mac-address-table filtering
Vlan    MAC Address    Type   Interface
------- ----------------- ------- -----------
 1    0000.2222.2222   FILTER Not available
```

Related Commands

Command	Description
mac-address-table filtering	Configure the filtering MAC address.

Platform N/A

Description

show mac-address-table interface

Use this command to show all the MAC address information of the specified interface including static and dynamic MAC address

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

Parameter Description

Parameter	Description
interface-id	Show the MAC address information of the specified Interface(physical interface or aggregate port).
vlan-id	Show the MAC address information of the VLAN.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mac-address-table interface
gigabitethernet 1/1
Vlan  MAC Address  Type   Interface
----- ------------- -------- ----------------
1   00d0.f800.1001 STATIC  gigabitethernet 1/1
1   00d0.f800.1002 STATIC  gigabitethernet 1/1
1   00d0.f800.1003 STATIC  gigabitethernet 1/1
1   00d0.f800.1004 STATIC  gigabitethernet 1/1
```

Related Commands

Command	Description
show mac-address-table static	Show the static MAC address.
show mac-address-table filtering	Show the filtering MAC address.
show mac-address-table dynamic	Show the dynamic MAC address.
show mac-address-table address	Show all types of MAC addresses.
show mac-address-table vlan	Show all types of MAC addresses of the specified VLAN.
show mac-address-table count	Show the address counts in the MAC address table.

Platform Description N/A

show mac-address-table notification

Use this command to show the MAC address notification configuration and the MAC address notification table.

show mac-address-table notification [**interface** [*interface-id*] **| history**]

Parameter Description

Parameter	Description
interface *interface-id*	Interface ID. Show the MAC address notification configuration on the interface.
history	Show the MAC address notification history.

Defaults

The MAC address notification configuration is shown by default.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie# show mac-address-table notification interface
Interface    MAC Added Trap MAC Removed Trap
---------    --------------   --------------
GigabitEthernet1/14  Disabled    Disabled
Ruijie# show mac-address-table notification
MAC Notification Feature: Disabled
Interval between Notification Traps: 1 secs
Maximum Number of entries configured in History Table:1
Current History Table Length: 0
Ruijie# show mac-address-table notification history
History Index: 0
MAC Changed Message:
Operation:ADD Vlan: 1 MAC Addr: 00f8.d012.3456 GigabitEthernet 3/1
```

Related Commands

Command	Description
mac-address-table notification	Enable MAC address notification.
snmp trap mac-notification	Enable the MAC address trap notification function on the specified interface.

Platform Description

N/A

show mac-address-table static

Use this command to show the static MAC address.

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

Parameter Description

Parameter	Description
mac-addr	Destination MAC address of the entry
vlan-id	VLAN ID of the entry

interface-id	Interface of the entry physical interface or aggregate port

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples Show only static MAC addresses

```
Ruijie# show mac-address-table static
Vlan   MAC Address     Type   Interface
---------- -------------------- -------- ---------
1  00d0.f800.1001  STATIC  gigabitethernet 1/1
1  00d0.f800.1002  STATIC  gigabitethernet 1/1
1  00d0.f800.1003  STATIC  gigabitethernet 1/1
```

Related Commands

Command	Description
mac-address-table static	Configure the static MAC address.

Platform Description N/A

show mac-address-table vlan

This command is used to display all addresses of the specified VLAN.

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

Parameter Description

Parameter	Description
vlan-id	VLAN ID

Defaults -

Command Mode Privileged EXEC mode

Usage Guide -

Configuration Examples

```
Ruijie# show mac-address-table vlan 1
Vlan  MAC Address    Type    Interface
----- -------------  ------- ------------------
1   00d0.f800.1001  STATIC  gigabitethernet 1/1
1   00d0.f800.1002  STATIC  gigabitethernet 1/1
1   00d0.f800.1003  STATIC  gigabitethernet 1/1
```

Related Commands

Command	Description
show mac-address-table static	This command is used to display static addresses.
show mac-address-table filtering	This command is used to display filtered addresses.
show mac-address-table dynamic	This command is used to display dynamic addresses.
show mac-address-table address	This command is used to display all address information about the specified address.
show mac-address-table interface	This command is used to display all address information about the specified interface.
show mac-address-table count	This command is used to display the number of addresses in the address table.

Platform Description

N/A

snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. You can use the **no** form of the command to disable this function.

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

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

Parameter Description

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

Defaults

Disabled.

Command Mode

Interface configuration mode.

Usage Guide

Use **show mac-address-table notification interface** to display configuration.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# snmp trap mac-notification added
```

Related Commands

Command	Description
mac-address-table notification	Enable MAC address notification.
show mac-address-table notification	Show the MAC address notification configuration and the MAC address notification table.

Platform Description

N/A

Aggregate Port Configuration Commands

aggregateport load-balance

Use this command to configure the load-balancing algorithm for an aggregate port (AP). Use the **no** form of this command to restore the default load-balancing configuration.

aggregateport load-balance { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-port** | **src-dst-ip-l4port** }

no aggregateport load-balance

Parameter Description

Parameter	**Description**
dst-mac	Traffic is distributed according to the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the packets with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
src-mac	Traffic is distributed according to the source MAC addresses of the incoming packets. For all the links of an aggregate port, the packets with different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-ip	Traffic is distributed according to the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links.
dst-ip	Traffic is distributed according to the destination IP addresses of the incoming packets. For all the links of an aggregate port, the packets with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Traffic is distributed according to the source IP addresses of the incoming packets. For all the links of an aggregate port, the packets with different addresses are distributed to different ports, and those with the same addresses are distributed to the same port.
src-dst-mac	Traffic is distributed according to the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.
src-port	Traffic is distributed according to the source port of the incoming packets. Packets with different source ports are forwarded through different ports, and the incoming packets with the same source port are load-balanced to the same outgoing port. If the source port is an AP member port, use the AP-ID to implement load-balancing. This means that packets with the same AP member port will be load-balanced to the same outgoing port.

src-dst-ip-l4port	Traffic is distributed according to the source IP, destination IP, source L4 port and destination L4 port. Packets with different source IP addresses, destination IP addresses, source L4 ports and destination L4 ports are forwarded through different ports, and packets with the same source IP address, destination IP address, source L4 port and destination L4 port are forwarded through the same port.

Defaults

Traffic is distributed according to the destination and source MAC addresses of the incoming packets.

Command Mode

Global configuration mode.

Usage Guide

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

Configuration Examples

Configure the MAC address-based load-balancing.

```
Ruijie(config)# aggregateport load-balance dst-mac
```

Related Commands

Command	**Description**
show aggregateport load-balance	Use this command to display aggregateport configurations.

Platform Description

N/A

port-group

Use this command to assign a physical interface as a member port of an aggregate port. Use the **no** form of the command to remove the membership from the aggregate port.

port-group *port-group-number*

no port-group

Parameter Description

Parameter	**Description**
port-group-number	Number of the member group of an aggregate port that is 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

This example shows how to specify the Ethernet interface 1/3 as members of AP 3:

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if)# port-group 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show aggregateport

Use this command to display the aggregate port configurations.

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

Parameter Description

Parameter	Description
aggregate-port-number	Interface number of the aggregate port.
load-balance	Show the load-balance algorithm on the aggregate port.
summary	Show the summary of the aggregate port.

Defaults

N/A

Command Mode

Any command modes.

Usage Guide

Information of all aggregate ports will be displayed unless you specify an interface number of the aggregate port.

Configuration Examples

See the configuration information of Aggregate Port 1.

```
Ruijie# show aggregateport 1 summary
AggregatePort  MaxPorts       SwitchPort Mode   Ports
------------------------------------------------------------------------
Ag1             8            Enabled     ACCESS
```

Related Commands

Command	Description
aggregateport load-balance	Configure a load-balancing algorithm for an AP.

Platform Description

N/A

LACP Configuration Commands

lacp system-priority

Use this command to set the LACP system priority. Use the **no** form of this command to restore the default setting.

lacp system-priority *system-priority*

no lacp system-priority

Parameter Description

Parameter	**Description**
system-priority	The LACP system priority, in the range of 0-65,535.

Defaults By default, the system priority is 32,768.

Command Mode Global configuration mode.

Usage Guide LACP system priority consists of the Layer2 management MAC address and its priority value, where the MAC address is fixed but the priority value is configurable. If two priorities are equal, then the smaller the MAC address is, the higher the priority is. All LACP groups on the switch share the system priority. Changing the system priority may influence the whole aggregation groups on the switch.

Configuration Examples

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

Related Commands

Command	**Description**
port-group *key* mode { active | passive }	Enable the LACP on the port and specify the aggregation group ID and operation mode.
lacp port-priority	Set the LACP port priority.

Platform Description N/A

port-group mode

Use this command to enable LACP and specify the group ID and the aggregation mode. Use the **no** form of this command to disable the LACP.

port-group *key* **mode** { **active** | **passive** }

no port-group

Parameter Description

Parameter	Description
key	Specify the group ID on the port to be aggregated. The key values vary with the aggregation group numbers supported for different products.
active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Defaults

By default, the LACP function is disabled on the interface.

Command Mode

Interface configuration mode.

Usage Guide

1 When multiple ports are to be aggregated, the ports with high priorities take precedence and the port with the highest priority is selected as the master port. The port priority sequence is determined according to the wire quality.

2 The LACP cannot be enabled on the ports with the function of forbidding the member ports to add to or leave the AP enabled; and the function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP member ports. The AP with the function of forbidding the member ports to add to or leave cannot configured as the LACP AP, and function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP AP.

3 The SYSLOG will be displayed when the LACP fails to leave the AP due to external function limitations, such as: %LACP-5-UNBUNDLE_FAIL: Interface FastEthernet 0/1 failed to leave the AggregatePort 1. In this case, please modify the configuration to cancel the related configuration of forbidding the member ports to leave the AP; otherwise the normal packets transmission on the AP will be influenced.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# port-group 1 mode active
```

Related Commands

Command	Description
port-group *key* **mode** { **active** | **passive** }	Enable the LACP on the port and specify the aggregation group ID and operation mode.

Platform Description

N/A

show lacp summary

Use this command to show the LACP aggregation information.

show lacp summary [*key*]

Parameter Description

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

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show LACP summary
Flags:S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
A - Device is in active mode.   P - Device is in passive mode.
Aggregate port 3:
Local information:
                  LACP port      Oper    Port    Port
Port   Flags    State    Priority    Key   Number  State
-------------------------------------------------------------
Gi0/1    SA       bndl       4096       0x3    0x1     0x3d
Gi0/2    SA       bndl       4096       0x3    0x2     0x3d
Gi0/3    SA       bndl       4096       0x3    0x3     0x3d
Partner information:
                  LACP port        Oper   Port    Port
Port   Flags    Priority   Dev ID    Key    Number  State
------------------------------------------------------------
Gi0/1   SA    61440   00d0.f800.0002   0x3   0x1    0x3d
Gi0/2   SA    61440   00d0.f800.0002   0x3   0x2    0x3d
Gi0/3   SA    61440   00d0.f800.0002   0x3   0x3    0x3d
```

Field	Description
Local information	Show the local LACP information.
Port	Show the system port ID.
Flags	Show the port state flag: “S” indicates that the LACP is stable and in the state of periodically sending the LACPPDU; “A” indicates that the port is in the active mode.

State	Show the port aggregation information: “bndl” indicates that the port is aggregated; “Down” represents the disconnection port state; “susp” indicates that the port is not aggregated.
LACP Port Priority	Show the LACP port priority.
Oper Key	Show the port operation key.
Port Number	Show the port number.
Port State	Show the flag bit for the LACP port state.
Partner information	Partly show the LACP information of the peer port.
Dev ID	Partly show the system MAC information of the peer device.

Related Commands

Command	**Description**
port-group *key* mode	Enable the LACP on the port and specify the aggregation group ID and operation mode.

Platform Description

N/A

VLAN Configuration 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.

Defaults

All layer-2 Ethernet interfaces are in the VLAN1.

Command mode

VLAN configuration mode.

Usage Guide

This command is only valid for the access port.

The configuration of this command is the same as specifying the VLAN to which interface belongs in the interface configuration mode (that is the **switchport access vlan** *vlan-id* command). For the two commands of adding the interface to the VLAN, the command configured later will overwrite the one configured before and take effect.

The configuration of adding the layer-2 AP into current VLAN through this command will only take effect for the layer-2 AP port, but not for the member port of the layer-2 AP port.

Configuration Examples

The following example adds the interface GigabitEthernet 0/10 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.

Platform Description N/A

dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode read-only

Use the command to set the max access mode of MIB node dot1qVlanIndex in the Dot1qVlanCurrentEntry list to **read-only**. Use the **no** form of this command to restore the max access mode to **deny access**.

dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode read-only

no dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Global configuration mode

Usage Guide You can return to privilege EXEC mode by executing the **end** command or pressing the key combination **Ctrl** and **C**.

Configuration Examples

The following example sets the max access mode of MIB node dot1qVlanIndex in the Dot1qVlanCurrentEntry list to **read-only**.

```
Ruijie(config)# dot1q-vlan-current-entry mib dot1q-vlan-index max-access mode
```

Related Commands

Command	Description
show vlan	Show member ports of the VLAN.

Platform Description

N/A

name

Use the command to specify the name of a VLAN. Use the **no** form of the command to restore the default setting.

name *vlan-name*

no name

Parameter Description

Parameter	Description
vlan-name	VLAN name

Defaults

The default name of a VLAN is the combination of “VLAN” and VLAN ID, for example, the default name of the VLAN 2 is “VLAN0002”.

Command mode

VLAN configuration Mode.

Usage Guide

You can view the VLAN settings by using the **show vlan** command.

Configuration Examples

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

Related Commands

Command	Description
show vlan	Show member ports of the VLAN.

Platform Description

N/A

show vlan

Show member ports of the VLAN.

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

Parameter Description

Parameter	Description
vlan-id	VLAN ID

Defaults Show all the information by default.

Command mode Privileged EXEC mode.

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

Configuration Examples

```
Ruijie# 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.

Platform Description N/A

switchport access

Use this command to configure an interface as a static access port and assign it to a VLAN. Use the **no** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter Description

Parameter	Description
vlan-id	The VLAN ID at which the port to be added.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command mode

Interface configuration mode.

Usage Guide

Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN.

If the port is a trunk port, the operation does not take effect.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	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.

Platform Description

N/A

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 an 802.1Q tunnel port.

Defaults

By default, the switch port is an access port.

Command mode

Interface configuration mode.

Usage Guide

If a switch port mode is access port, it can be the member port of only one VLAN. Use the **switchport access vlan** command to specify the member of the VLAN.

A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed

VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use the **switchport trunk** command to define the allowed-VLANs list.

Configuration Examples

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

Related Commands

Command	Description
switchport access	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.

Platform Description

N/A

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, and 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.

Defaults

The default allowed-VLAN list is all the VLANs, the default native VLAN is VLAN 1.

Command mode

Interface configuration mode.

Usage Guide

Native VLAN:

A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged.

Allowed-VLAN List:

By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk port by configuring allowed VLAN lists on a trunk port .

Use the **show interfaces switchport** command to display configuration.

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 static access port and assign it to a VLAN.

Platform Description

N/A

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.

Defaults

N/A

Command mode

Global configuration mode.

Usage Guide

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

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

Configuration Examples

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

Related Commands

Command	Description
show vlan	Show member ports of the VLAN.

Platform Description

N/A

Protocol VLAN Configuration Commands

protocol-vlan profile (in global configuration mode)

Use this command to configure message type and Ethernet type profile.

protocol-vlan profile *num* **frame-type** *type* **ether-type** *type*

Use this command to delete the specified profile.

no protocol-vlan profile *num*

Use this command to delete all profiles.

no protocol-vlan profile

Parameter Description

Parameter	Description
num	Profile indexes
type	Type of message and Ethernet

Defaults N/A

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# protocol-vlan  profile 1 frame-type
ETHERII ether-type aarp
```

Related Commands

Command	Description
show protocol-vlan profile	N/A
show protocol-vlan profile *num*	N/A
no protocol-vlan profile	N/A
no protocol-vlan profile *num*	N/A

Platform Description N/A

protocol-vlan profile (in interface configuration mode)

Use this command to apply some profile to an interface.

protocol-vlan profile *num* **vlan** *id*

Clear the specified profile on the port.

no protocol-vlan profile *id*

Clear all profiles on the port.

no protocol-vlan profile

Parameter Description

Parameter	Description
num	Profile indexes
id	VLAN ID, the maximal VLAN the product supports.

Defaults N/A

Command mode Interface configuration mode.

Usage Guide N/A

Configuration Examples

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

Related Commands

Command	Description
show protocol-vlan profile	N/A
show protocol-vlan profile *num*	N/A
no protocol-vlan profile	N/A
no protocol-vlan profile *num*	N/A

Platform Description N/A

show protocol-vlan

Show the configuration of protocol VLAN.

show protocol-vlan

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration

```
Ruijie# show protocol-vlan
```

Examples

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Private VLAN Configuration Commands

private-vlan association

Use this command to associate the secondary VLAN with the primary command.

private-vlan association { *svlist* | **add** *svlist* | **remove** *svlist* }

no private-vlan association

Parameter Description

Parameter	Description
svlist	The secondary VLAN list
no	Removes the association between the primary VLAN and all the secondary VLANs.

Defaults No association.

Command mode Primary VLAN configuration Mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan association add 24-26
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description N/A

private-vlan mapping

Use this command to map the secondary VLAN to the L3 SVI interface.

private-vlan mapping { *svlist* | **add** *svlist* | **remove** *svlist* }

no private-vlan mapping

Parameter Description

Parameter	Description
svlist	Secondary VLAN list
no	Deletes the mapping.

Defaults N/A

Command mode The interface mode corresponding to the primary VLAN

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# interface vlan 22
Ruijie(config-if)# private-vlan mapping add 24-26
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description N/A

private-vlan *type*

Use this command to configure the VLAN as the private VLAN.

private-vlan { **community | isolated | primary** }

no private-vlan { **community | isolated | primary** }

Parameter Description

Parameter	Description
community	Configures it as the community VLAN.
isolated	Configures it as the isolated VLAN.
primary	Configures it as the primary VLAN.
no	Deletes the corresponding private VLAN configuration.

Defaults No private VLAN is configured.

Command mode VLAN configuration Mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan primary
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description

N/A

switchport mode private-vlan

Use this command to declare the private VLAN mode of the interface.

switchport mode private-vlan { **host** | **promiscuous** }

no switchport mode

Parameter Description

Parameter	Description
host	Host mode of the private VLAN
promiscuous	Promiscuous mode of the private VLAN
no	Deletes the private VLAN configuration of the port.

Defaults

N/A

Command mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

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

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description

N/A

switchport private-vlan association trunk

Use this command to associate the trunk port in the private VLAN mode, which is associated with the primary VLAN and the secondary VLAN.

switchport private-vlan association trunk *p_vid s_vid*

no switchport private-vlan association trunk

Parameter Description

Parameter	Description
p_vid	Primary VID.
s_vid	Secondary VID

no	Deletes the host port from the private VLAN.

Defaults

N/A

Command mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan association trunk 202 203
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

switchport private-vlan host-association

Use this command to associate the primary VLAN, which is associated with the private VLAN mode of the interface, with the secondary VLAN.

switchport private-vlan host-association *p_vid s_vid*

no switchport private-vlan host-association

Parameter Description

Parameter	**Description**
p_vid	Primary VID.
s_vid	Secondary VID
no	Deletes the host port from the private VLAN.

Defaults

N/A

Command mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode private-vlan host
Ruijie(config-if)# switchport private-vlan host-association 22 23
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description

N/A

switchport private-vlan mapping

Use this command to configure the promiscuous secondary VLANs that the promiscuous mode of the private VLAN maps.

switchport private-vlan mapping *p_vid* { *svlist* | **add** *svist* | **remove** *svlist* }

no switchport private-vlan mapping

Parameter Description

Parameter	Description
p_vid	Primary VID
svlist	Secondary VLAN list.
no	Removes all the promiscuous secondary VLANs.

Defaults

No promiscuous secondary VLAN is configured.

Command mode

Hybrid interface configuration mode of private VLAN

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode private-vlan
promiscuous
Ruijie(config-if)# switchport private-vlan mapping 22 add 23-25
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform Description

N/A

switchport private-vlan promiscuous trunk

Use this command to configure the ports as a promiscuous trunk port, which is associated with the L2 port and the private VLAN. Multiple pairs are allowed to associate.

switchport private-vlan promiscuous trunk *p_vid_s_list*

no switchport private-vlan promiscuous trunk *p_vid_s_list*

Parameter Description

Parameter	**Description**
p_vid	Primary VID
svlist	Secondary VLAN list.
no	Removes all the relationships between the layer-2 ports and private VLANs.

Defaults N/A

Command mode Interface configuration mode

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# switchport private-vlan promiscuous trunk 202 203
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

show vlan private-vlan

Show the configuration of private VLAN.

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

Parameter Description

Parameter	**Description**
primary	Shows the primary VLAN information.
community	Shows the community VLAN information.
isolated	Shows the isolated VLAN information.

Defaults No private VLAN is configured.

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

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

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

switchport hybrid allowed vlan

Use this command to configure the output rules of a hybrid port.

switchport hybrid allowed vlan [[**add**] [**tagged** | **untagged**] | **remove**] v*list*

no switchport hybrid allowed vlan

Parameter Description

Parameter	Description
no	Restores the output rules of the hybrid port to the default settings.

Defaults

No output rules are configured.

Command mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie(config-if)# switchport hybrid allowed vlan add untagged 3-5
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

switchport hybrid native vlan

Use this command to configure the default VLAN of a hybrid port.

switchport hybrid native vlan *vid*

no switchport hybrid native vlan

Parameter Description

Parameter	Description
no	Restores the hybrid port to the default VLAN.

Defaults No default VLAN is configured.

Command mode Interface configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config-if)# switchport hybrid native vlan 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

switchport mode hybrid

Use this command to configure the port as a hybrid port.

switchport mode hybrid

no switchport mode

Parameter Description

Parameter	Description
no	Deletes the hybrid port.

Defaults No hybrid port is configured.

Command mode Interface configuration mode.

Usage Guide N/A

Configuration Examples

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

Related

Command	Description

Commands

N/A	N/A

Platform Description

N/A

Share VLAN Configuration Commands

share

Use this command to set the share vlan.

N/A

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode VLAN configuration mode.

Usage Guide Use the **no share** command to cancel the share vlan.

Enter the **end** command or **Ctrl+C** to return to the privileged EXEC mode.

Enter the **exit** command to return to the global configuration mode.

Configuration Examples

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)# share
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mac-address-table share

Use this command to show the mac address status: original, duplicated and null. The “null” item indicates that share vlan has not been configured.

show mac-address-table share

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode

Any configuration mode.

Usage Guide

Enter the **end** command or **Ctrl+C** to return to the privileged EXEC mode.

Enter the **exit** command to return to the global configuration mode.

Configuration Examples

```
Ruijie# show mac-address-table share
Vlan  MAC Address     Type   Interface   Status
----  -------------- ------- ----------- ----------
   1  0040.4650.1e1e DYNAMIC Gigabit 0/1 original
   2  0040.4650.1e1e DYNAMIC Gigabit 0/1 duplicated
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Voice VLAN Configuration Commands

show voice vlan

Use this command to view the Voice VLAN configurations and the current state, including the working mode of the port with Voice VLAN enabled.

show voice vlan

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie(config)# show voice vlan
Voice VLAN status: ENABLE
Voice VLAN ID: 2
Voice VLAN security mode: Security
Voice VLAN aging time: 5 minutes
Voice VLAN cos: 6
Voice VLAN dscp: 46
Current voice vlan enabled port mode:
PORT                    MODE
----------------------------------------------------
Fa0/1                   Auto
```

Related commands

Command	Description
voice vlan *vlan-id*	Set a voice vlan.
voice vlan aging *minutes*	Set the Voice VLAN aging time.
voice vlan cos *cos-value*	Set the CoS value for the Voice VLAN.

voice vlan dscp *dscp-value*	Set the DSCP value for the Voice VLAN.
voice vlan enable	Enable the Voice VLAN.
voice vlan mode auto	Set the Voice VLAN working mode.
voice vlan security enable	Enable the Voice VLAN security mode.

show voice vlan oui

Use this command to view the OUI address, OUI mask and the description information.

show voice vlan oui

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie(config)# show voice vlan oui
OUI             Mask            Description
--------------- --------------- ---------------
0001.e300.0000  ffff.ff00.0000  Siemens phone
0003.6b00.0000  ffff.ff00.0000  Cisco phone
0004.0d00.0000  ffff.ff00.0000  Avaya phone
0060.b900.0000  ffff.ff00.0000  Philips/NEC phone
00d0.1e00.0000  ffff.ff00.0000  Pingtel phone
00e0.7500.0000  ffff.ff00.0000  Polycom phone
00e0.bb00.0000  ffff.ff00.0000  3com phone
```

The following lists the field description :

Field	Description

OUI	The OUI address, the source MAC address for the voice packet.
Mask	The OUI mask. The valid length for the OUI address.
Description	The description information for the OUI address.

Related commands

Command	Description
voice vlan mac-address *mac-addr* **mask** *oui-mask* **[description** *text***]**	Set the OUI address for the voice packet recognized by the Voice VLAN.

voice vlan

Use this command to enable Voice VLAN in the global configuration mode. Use the **no** form of this command to disable this function.

voice vlan *vlan-id*

no voice vlan

Parameter description

Parameter	Description
vlan-id	The Voice VLAN ID.

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

Use this command to enable the Voice VLAN and specify the Voice Vlan ID.

Caution:

1) The corresponding VLAN shall be created before configuring the Voice VLAN;
2) The default VLAN is VLAN1 and cannot be set as the Voice VLAN;
3) A VLAN is not allowed to be set as the Voice VLAN and the Super VLAN at the same time;

4) With 802.1x VLAN auto-switching function enabled, the assigned VID shall not be set as the Voice VLAN ID;
5) RSPAN Remote VLAN and Voice VLAN cannot be the same VLAN, or it influences the remote port mirror and the Voice VLAN function.

Examples

The following example shows how to set the VLAN2 as the Voice VLAN:

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

Related commands

Command	Description
show voice vlan	Show Voice VLAN configurations and the current state.

voice vlan aging

Use this command to set the Voice VLAN aging time in the global configuration mode. Use the **no** form of this command to restore it to the default value.

voice vlan aging *minutes*

no voice vlan aging

Parameter description

Parameter	Description
minutes	The Voice VLAN aging time.

Default Settings

1440 minutes

Command mode

Global configuration mode.

Usage guidelines

If the device has not received any voice packets from the port within the aging time, this Voice VLAN will be removed from this port.

Note

The aging time is valid for the auto-mode only.

Examples

The following example shows how to set the Voice VLAN aging time as 10 minutes:

```
Ruijie(config)# voice vlan aging 10
```

Related commands

Command	Description
show voice vlan	Show Voice VLAN configurations and the current state.

voice vlan cos

Use this command to set the Voice VLAN CoS value in the global configuration mode. Use the **no** form of this command to restore it to the default value.

voice vlan cos *cos-value*

no voice vlan cos

Parameter description

Parameter	Description
cos-value	The Voice VLAN CoS value.

Default Settings

6

Command mode

Global configuration mode.

Usage guidelines

You can improve the Voice VLAN priority level and the session quality, by modifying the Voice VLAN CoS and DSCP value.

Examples

The following example shows how to set the Voice VLAN CoS value as 5:

```
Ruijie(config)# voice vlan cos 5
```

Related commands

Command	Description
show voice vlan	Show Voice VLAN configurations and the current state.

voice vlan dscp

Use this command to set the Voice VLAN DSCP value in the global configuration mode. Use the **no** form of this command to restore it to the default value.

voice vlan dscp *dscp-value*

no voice vlan dscp

Parameter description

Parameter	Description
dscp-value	The Voice VLAN CoS value.

Default Settings

46

Command mode

Global configuration mode.

Usage guidelines

You can improve the Voice VLAN priority level and the session quality, by modifying the Voice VLAN CoS and DHCP value.

Examples

The following example shows how to set the Voice VLAN DSCP value as 40:

```
Ruijie(config)# voice vlan dscp 40
```

Related commands

Command	Description
show voice vlan	Show Voice VLAN configurations and the current state.

Platform description

voice vlan enable

Use this command to enable the Voice VLAN DSCP value in the interface configuration mode. Use the **no** form of this command to disable this function.

voice vlan enable

no voice vlan enable

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Interface configuration mode.

Usage guidelines

Use this command to enable the Voice VLAN on the physical port only. The Voice VLAN can be enabled on the Access Port, Trunk Port, Hybrid Port, Private VLAN host port, Private VLAN promiscuous port and Uplink port on the Ruijie products.

📖 **Note**

With the global Voice VLAN disabled, although the Voice VLAN can be enabled on the port, it is invalid.

Examples

The following example shows how to enable the Voice VLAN function on the interface FastEthernet 0/1:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# voice vlan enable
```

Related commands

Command	Description
show voice vlan	Show Voice VLAN configurations and the current state.

voice vlan mac-address

Use this command to set the recognizable Voice VLAN OUI address. Use the **no** form of this command to remove the OUI address.

voice vlan mac-address *mac-addr* **mask** *oui-mask* **[description** *text***]**

no voice vlan mac-address *mac-addr*

Parameter description

Parameter	Description
mac-addr	In the format of *H.H.H.* The source MAC address for the voice packets.
oui-mask	In the format of *H.H.H.* The valid length for the OUI address.
text	The description for the OUI address.

Default Settings

By default, no OUI has been configured.

Command mode

Global configuration mode.

Usage

Use this command to identify the voice packets from

guidelines

different manufacturers. The first three bytes of the MAC address for the voice device are used to identify the manufacture. Voice VLAN determines whether the packets are voice packets or not through the OUI address obtained from the source MAC address and the OUI mask for the received packets.

Note

The Voice VLAN OUI address cannot be the multicast address and the configured mask shall be continuous.

Examples

The following example shows how to set the OUI address 0012.3400.0000 as the valid address for the Voice VLAN:

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
```

Related commands

Command	Description
show voice vlan oui	Show the OUI address, OUI address mask and the descriptions.

voice vlan mode auto

Use this command to set the Voice VLAN auto mode in the interface configuration mode. Use the **no** form of this command to cancel the Voice VLAN auto mode.

voice vlan mode auto

no voice vlan mode auto

Parameter description

Parameter	Description
-	-

Default Settings

Auto mode.

Command mode

Interface configuration mode.

Usage guidelines

The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.

Caution

1. With the Voice VLAN enabled on the port and in the manual mode, this port must be added to the Voice VLAN manually to ensure the function validity.
2. When the port works in the auto-mode, note that the native VLAN of the port cannot be set as the Voice VLAN for the normal function performance.
3. The Trunk Port/Hybrid Port on the Ruijie product can transmit the packets in all VLANs by default. First remove the Voice VLAN from the allowed VLAN list for the port, then enable the Voice VLAN to ensure that the port disconnecting with the voice device cannot be added to the Voice VLAN, or the port not used for a long time can be still in the Voice VLAN.

Note

1. With the Voice VLAN enabled on the port, the auto and manual modes switchover is disallowed. Disable the Voice VLAN first if it is necessary to switch the modes.
2. In the auto mode, it fails to add/remove the port to/from the Voice Vlan by using the command.

Examples

The following example shows how to set the Voice VLAN on the interface FastEthernet 0/1 work in the auto mode:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-vlan)# voice vlan mode auto
```

Related commands

Command	Description
show voice vlan	Show Voice VLAN configurations and the current state.

voice vlan security enable

Use this command to enable the Voice VLAN security mode in the global configuration mode. Use the **no** form of this command to disable the security mode.

voice vlan security enable

no voice vlan security enable

Parameter description

Parameter	Description
-	-

Default Settings

Enabled

Command mode

Global configuration mode.

Usage guidelines

The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.

Caution

You are not recommended to transmit the voice and service data in the Voice VLAN at the same time. But if it is necessary for you, you shall ensure that the Voice VLAN security mode has been disabled.

Note

In the security mode, only the source MAC addresses for the untagged packets and the packets carried with Voice VLAN tag are checked. For other packets carried with non-voice vlan tag that free from the Voice VLAN security/normal mode, the devices forward or discard those packets according to the VLAN rule.

Examples

The following example shows how to enable the Voice VLAN security mode:

```
Ruijie(config)# voice vlan security enable
```

Related commands

Command	Description
show voice vlan	Show Voice VLAN configurations and the current state.

MAC VLAN Configuration Commands

mac-vlan enable

Use this command to enable the MAC VLAN function on the port in interface configuration mode.

mac-vlan enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command mode Interface configuration mode.

Usage Guide The MAC VLAN entries configured globally won't take effect on the port unless the MAC VLAN function is enabled on this port.

The MAC VLAN function can be enabled on the hybrid port only.

Configuration Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/10
Ruijie(config-if)# mac-vlan enable
Ruijie(config-if)# no mac-vlan enable
Ruijie(config-if)# end
```

Related Commands

Command	Description
show mac-vlan interface	Shows the MAC-VLAN enabled port list.

Platform Description N/A

mac-vlan mac-address

Use this command to configure the static MAC VLAN entries manually in global configuration mode.

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri_val*]

Parameter Description

Parameter	Description
mac-address *mac-address*	Specifies the MAC address.

mask *mac-mask*	Specifies the MAC address mask, with the high bits being all 1 in binary. This field is full of Fs by default.
vlan *vlan-id*	Specifies the VLAN corresponding to the MAC address, in the range of 1 to 4,094.
priority *pri_val*	Specifies the 802.1p priority of the VLAN corresponding to the MAC address, in the range of 0 to 7. The default value is 0.

Defaults

No static MAC-VLAN entry is configured by default.

Command mode

Global configuration mode.

Usage Guide

The **mac-vlan mac-address** command is used to configure the VLAN corresponding to the MAC address and its priority. The **no mac-vlan** command is used to delete the relationship between the MAC address and VLAN.

Configuration Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# mac-vlan mac-address 0001.0001.0001 vlan 100
priority 3
Ruijie(config)# mac-vlan mac-address 0002.0002.0000 mask
ffff.ffff.0000 vlan 200 priority 5
Ruijie# show mac-vlan all
The following MAC VLAN address exist:
S: Static   D: Dynamic
MAC ADDR         MASK            VLAN ID   PRIO   STATE
-------------------------------------------------------
0002.0002.0000   ffff.ffff.0000   200       5      S
0001.0001.0001   ffff.ffff.ffff   100       3      S
Total MAC VLAN address count: 2
```

Related Commands

Command	Description
show mac-vlan all	Shows the MAC-VLAN entries.

Platform Description

N/A

show mac-vlan

Use this command to show the MAC-VLAN entries configured.

show mac-vlan

Parameter Description

Parameter	Description

all	Shows all MAC-VLAN entries.
dynamic	Shows the MAC-VLAN entries configured dynamically.
static	Shows the MAC-VLAN entries configured statically.
mac-address *mac-address*	Shows the MAC-VLAN entries in MAC.
mask *mac-mask*	Shows the MAC-VLAN entries in the specified MAC address range.
vlan *vlan-id*	Shows the MAC-VLAN entries of the specified VLAN.

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

If the parameter **mac-address** is specified without the parameter **mask**, the MAC-VLAN entry of the single MAC address is shown.

If the parameters **mac-address** and **mask** are both specified, the MAC-VLAN entries in the specified MAC address range are shown.

Configuration Examples

```
Ruijie# show mac-vlan all
The following MAC VLAN addresses exist:
S: Static   D: Dynamic
MAC ADDR          MASK           VLAN ID   PRIO   STATE
-------------------------------------------------------
0011.1100.0000   ffff.ff00.0000   100      1     S
0022.2222.0000   ffff.ffff.0000   200      2     S
0000.0000.0003   ffff.ffff.ffff   300      3     D
0000.0000.0004   ffff.ffff.ffff   400      4     D
0000.0000.0005   ffff.ffff.ffff   500      5     S&D
0000.0000.0006   ffff.ffff.ffff   600      6     S
0000.0000.0007   ffff.ffff.ffff   700      7     S&D
Total MAC VLAN address count: 7
```

Related Commands

Command	Description
mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri_val*]	Configures the static MAC VLAN entries.

Platform Description

N/A

show mac-vlan interface

Use this command to show the MAC-VLAN enabled port list.

show mac-vlan interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

With the MAC VLAN function enabled on the port, use this command to verify whether the configuration is successful.

Configuration Examples

```
Ruijie# show mac-vlan interface
MAC VLAN is enabled on following interface:
  ---------------------------------------
  fastethernet 0/3
  fastethernet 0/10
```

Related Commands

Command	Description
mac-vlan enable	Enables the MAC VLAN function on the port.

Platform Description

N/A

MSTP Configuration Commands

bpdu src-mac-check

This command is used to enable the BPDU source MAC address check function on an interface. Use the **no** option of this command to disable the function.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

Parameter Description

Parameter	Description
H.H.H	Indicates that only the BPDU frames from this MAC address are received.
no	Indicates that the BPDU frames from any MAC address are received.

Defaults Disabled

Command Mode Interface configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

Command	Description
-	**-**

Platform Description **-**

clear spanning-tree counters

This command is used to clear statistics of STP receiving/transmitting packets.

clear spanning-tree counters [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	ID of the corresponding interface

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide -

Configuration Examples

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

Related Commands

Command	Description
show spanning-tree counters	Show statistics of STP receiving/transmitting packets.

Platform Description -

clear spanning-tree detected-protocols

This command is used to force the interface to send the RSTP BPDU frames and check the BPDU frames.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	ID of the corresponding interface

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide -

Configuration Examples

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

Related Commands

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

Platform Description -

show spanning-tree

This command is used to display the global spanning-tree configurations.

show spanning-tree [**summary** | **forward-time** | **hello-time** | **max-age** | **inconsistentports |** **tx-hold-count** | **pathcost method** | **max_hops | counters**]

Parameter Description

Parameter	Description
summary	Show the information of MSTP instances and forwarding status of their interfaces.
inconsistentports	Show the blocked port due to root guard or loop guard.
forward-time	Show BridgeForwardDelay.
hello-time	Show BridgeHelloTime.
max-age	Show BridgeMaxAge.
max-hops	Show the maximum hops of an instance.
tx-hold-count	Show TxHoldCount.
pathcost *method*	Show the method used for calculating path cost.
counters	Show statistics of STP receiving/transmitting packets.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

-

Configuration Examples

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

Related Commands

Command	Description
spanning-tree pathcost method	Set the pathcost calculation method.
spanning-tree forward-time	Set BridgeForwardDelay.
spanning-tree hello-time	Set BridgeHelloTime.
spanning-tree max-age	Set BridgeMaxAge.
spanning-tree max-hops	Set the maximum hops of an instance.
spanning-tree tx-hold-count	Show TxHoldCount.

Platform Description

-

show spanning-tree interface

This command is used to show the STP configuration of the interface, including the optional spanning tree configuration.

show spanning-tree interface *interface-id* [{ **bpdufilter** | **portfast** | **bpduguard** | **link-type** }]

Parameter Description

Parameter	Description
interface-id	Interface ID

bpdufilter	Show the status of BPDU filter.
portfast	Show the status of portfast.
bpduguard	Show the status of BPDU guard.
link-type	Show the link type of an interface.

Defaults -

Command Mode Privileged EXEC mode

Usage Guide -

Configuration Examples

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

Related Commands

Command	Description
spanning-tree bpdufilter	Enable the BPDU filter feature on an interface.
spanning-tree portfast	Enable the portfast on an interface.
spanning-tree bpduguard	Enable the BPDU guard on an interface.
spanning-tree link-type	Set the link type of an interface to point-to-point.

Platform Description **-**

show spanning-tree mst

This command is used to display the configuration of MST and the information about instances in privileged EXEC mode.

show spanning-tree mst { **configuration** | *instance-id* [**interface** *interface-id*] }

Parameter Description

Parameter	Description
configuration	The MST configuration of the device.
instance-id	Instance ID
interface-id	Interface ID

Defaults All the instances are displayed by default.

Command Mode Privileged EXEC mode.

Usage Guide -

Configuration Examples

```
Ruijie# show spanning-tree mst configuration
```

Related Commands

Command	Description
spanning-tree mst configuration	Enter the MST region configuration.
spanning-tree mst cost	Show the path cost of the instance.
spanning-tree mst max-hops	Show the maximum hops of the instance.
spanning-tree mst priority	Show the device priority of the instance.
spanning-tree mst port-priority	Show the port priority of the instance.

Platform Description

-

spanning-tree

This command is used to enable MSTP and configure its basic settings globally. The **no** option of the command disables the spanning-tree function. The **no** option 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
hello-time *seconds*	Interval at which the device sends the BPDU message
max-age *seconds*	Maximum aging time of the BPDU message

Defaults

Disabled

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 as shown below:

2*(Hello Time+1.0snd) <= Max-Age Time <= 2*(Forward-Delay–1.0snd)

If the values do not meet the condition, the settings will fail.

Configuration Examples

Example 1: Enable the spanning-tree function:

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

Example 2: Configure the BridgeForwardDelay:

```
Ruijie(config)# spanning-tree  forward-time 10
```

Related Commands

Command	Description
show spanning-tree	Show the global STP configuration.
spanning-tree mst cost	Set the PathCost of an STP interface.

spanning-tree tx-hold-count STP	Set the global TxHoldCount of STP.

Platform Description -

spanning-tree autoedge

This command is used to enable Autoedge on an interface. You can use the **disabled** option of this command to disable Autoedge on the interface.

spanning-tree autoedge [**disabled**]

Parameter Description

Parameter	Description
disabled	Disable the Autoedge of an interface.

Defaults Enabled

Command Mode Interface configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

Command	Function
show spanning-tree interface	Show the STP configuration information of an interface.

Platform Description -

spanning-tree bpdufilter

This command is used to enable the BPDU filter function on an 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 bpduguard [**enabled** | **disabled**]

Parameter Description

Parameter	Description
enabled	Enable the BPDU filter on an interface.
disabled	Disable the BPDU filter on an interface.

Defaults Disabled

Command Mode Interface configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

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

Platform Description -

spanning-tree bpduguard

This command is used to enable the BPDU guard function on an 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	Enable BPDU guard on an interface.
disabled	Disable BPDU guard on an interface.

Defaults Disabled

Command Mode Interface configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

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

Platform Description -

spanning-tree compatible enable

This command is used to send the message selectively carried with MSTI according to the interface attributes of current port to realize interconnection with other products.

spanning-tree compatible enable

no spanning-tree compatible enable

Parameter Description

Parameter	Description
-	-

Defaults

Disabled

Command Mode

Interface configuration mode

Usage Guide

-

Configuration Examples

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

Related Commands

Command	Description
-	-

Platform Description

-

spanning-tree guard loop

This command is used to enable **loop guard** on an interface to prevent the root port or backup port from generating loop as the result that they cannot receive bpdu. You can use the **no** option of this command to disable the **loop guard**.

spanning-tree guard loop

no spanning-tree guard loop

Parameter Description

Parameter	Description
-	-

Defaults

Disabled

Command Mode

Interface configuration mode

Usage Guide

-

Configuration Examples

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

Related Commands

Command	Description
-	-

Platform Description **-**

spanning-tree guard none

This command is used to disable the **guard** on an interface. You can use the **no** option of this command to disable the **guard** on the interface.

spanning-tree guard none

no spanning-tree guard none

Parameter Description

Parameter	Description
-	-

Defaults Disabled

Command Mode Interface configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

Command	Description
-	**-**

Platform Description **-**

spanning-tree guard root

This command is used to enable the **root guard** on an interface to prevent the change of current root bridge position because of error configuration and illegal message attacks. You can use the **no** option of this command to disable the **root guard** on the interface.

spanning-tree guard root

no spanning-tree guard root

Parameter Description

Parameter	Description
-	-

Defaults Disabled

Command Mode Interface configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

Command	Description
-	-

Platform Description -

spanning-tree ignore tc

This command is used to enable the tc filtering switch on an interface. You can use the **no** option of this command to disable the tc filtering switch on the interface. With tc filtering enabled, the TC messages received on the interface will not be processed.

spanning-tree ignore tc

no spanning-tree ignore tc

Parameter Description

Parameter	Description
-	-

Defaults By default, the TC filtering function is disabled.

Command Mode Interface configuration mode

Configuration Examples

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

Related Commands

Command	Description
-	-

Platform Description -

spanning-tree link-type

This command is used to configure the link type of the interface to “point to point”. You can use the **no** option of the command to restore the default configuration.

spanning-tree link-type [**point-to-point** | **shared**]

no spanning-tree link-type

Parameter

Parameter	Description

Description

point-to-point	Forcibly set the link type of the interface to point-to-point.
shared	Forcibly set the link type of the interface to shared.

Defaults

For a full-duplex interface, its link type is point-to-point link by default; for a half-duplex interface, its link type is shared by default.

Command Mode

Interface configuration mode

Usage Guide

-

Configuration Examples

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

Related Commands

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

Platform Description

-

spanning-tree loopguard default

This command is used to enable **loop guard** globally to prevent the root port or backup port from generating loops as the result that they cannot receive bpdu. You can use the **no** form of this command to disable the **loop guard**.

spanning-tree loopguard default

no spanning-tree loopguard default

Parameter Description

Parameter	Description
-	-

Defaults

Disabled

Command Mode

Global configuration mode

Usage Guide

-

Configuration Examples

```
Ruijie(config)# spanning-tree loopguard default
```

Related Commands

Command	Description
-	**-**

Platform Description -

spanning-tree max-hops

This command is used to set the maximum number of hops (Max-hops Count) of the BPDU frame in the global configuration mode and the number of devices in a region that the BPDU frame passes before being dropped. This parameter applies to all instances. You can use the **no** option of the 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 frame passes the device before being dropped, which ranges from 1 to 40.

Defaults The default is 20 hops.

Command Mode Global configuration mode

Usage Guide

In the region, the BPDU frame sent by the root bridge includes a Hot Count field. When the BPDU frame passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates timeout of the BPDU message. The device will drop the BPDU with the Hop Count of 0.

Changing the **max-hops** affects all instances.

Configuration Examples

This example shows how to set the max-hops of the spanning tree to 10 for all MST instances:

```
Ruijie(config)# spanning-tree  max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** command in privileged EXEC mode.

Related Commands

Command	Description
show spanning-tree	Show the MSTP information.

Platform Description -

spanning-tree mode

This command is used to set the STP version in the global configuration mode. You can use the **no** option of the command to restore the default version of the spanning-tree.

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

MSTP version

Command Mode

Global configuration mode

Usage Guide

-

Configuration Examples

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

Related Commands

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

Platform Description

-

spanning-tree mst configure

This command is used to enter the MST configuration mode in the global configuration mode and configure the MSTP region. You can use the **no** option of the command to restore all parameters (name, revision, vlan map) to default.

spanning-tree mst configuration

no spanning-tree mst configuration

Parameter Description

Parameter	Description
-	-

Defaults

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

Command Mode

Global configuration mode

Usage Guide

To return to the privileged EXEC mode, enter **end** or **press Ctrl+C.**

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

After entering the MST configuration mode, you can use the following commands to configure parameters:

instance *instance-id* **vlan** *vlan-range*: Adds the VLANs to the MST instance. The range of *instance-id* is 0 to 64 and the range of VLAN is 1 to 4095. The *vlan-range* can be a set of some inconsecutive VLANs separated with comma or some consecutive VLANs in the form of start VLAN number–end VLAN number. For example, **instance 10 vlan 2,3,6-9** means that VLANs 2, 3, 6, 7, 8, 9 are added to instance 10. By default, all VLANs are in Instance 0. To remove a VLAN from an instance, use the **no** option of the command: **no instance** *instance-id* [**vlan** *vlan-range*]. (In this case, the range of instance is 1 to 64).

You are advised to control the number of instances created in a pile.

name *name*: Specify the MST name, a string of up to 32 characters. You can use the **no name** command to restore the default setting.

revision *version*: Set the MST version which ranges from 0 to 65535. You can use the **no name** command to restore the default setting.

show spanning-tree mst configuration: Shows the information of the current MST region.

Configuration Examples

This example shows how to enter the MST configuration mode, and map VLANs 3, 5 to 10 to MST instance 1:

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan  3, 5-10
Ruijie(config-mst)# name region 1
Ruijie(config-mst)# revision  1
Ruijie(config-mst)# show spanning-tree mst configuration
MST configuration
Name [region1]
Revision 1
Instance  Vlans Mapped
----------  ---------------------
0       1-2,4,11-4094
1       3,5-10
-----------------------------------
Ruijie(config-mst)# exit
Ruijie(config)#
```

To remove VLAN 3 from instance 1, execute this command after entering the MST configuration mode:

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

Use the following demand to delete instance 1:

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

You can verify the above with the **show** command of the MST configuration commands.

Related Commands

Command	Description
show spanning-tree mst	Show the MST region configuration.
instance *instance-id* **vlan** *vlan-range*	Add VLANs to the MST instance.

name	Configure the name of MST.
revision	Configure the version number of MST.

Platform Description -

spanning-tree mst cost

This command is used to set the path cost of each instance in the interface configuration mode. You can 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 of 0 to 64
cost	Path cost in the range of 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 shows how to set the path cost to 400 on an 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 privileged EXEC mode.

Related Commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst port-priority	Configure the priority of an interface.
spanning-tree mst priority	Configure the priority of an instance.

Platform Description -

spanning-tree mst port-priority

This command is used to configure the interface priority for different instances of an interface in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. You can use the **no** option of the 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, for which sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 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 a higher priority will be in charge of forwarding. If all interfaces have the same priority, the interface with a smaller number will be in charge of the forwarding.

Configuration Examples

This example shows how to set 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 privileged command "**show spanning-tree mst** *instance-id* "

Related Commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst cost	Set the path cost.
spanning-tree mst priority	Set the device priority for different instances.

Platform Description -

spanning-tree mst priority

This command is used to set the device priority for different instances in the global configuration mode. You can use the **no** option of the 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, for which sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152,53248, 57344 and 61440, all of which are multiples of 4096.

Defaults

The default instance ID is 0.

The default device priority is 32768.

Usage Guide

-

Command Mode

Global configuration mode

Configuration Examples

The following example sets the device priority of Instance 20 to 8192.

```
Ruijie(config-if)# spanning-tree mst 20 priority 8192
```

You can verify your settings by entering the privileged command "**show spanning-tree mst** instance **interface** *instance-id*".

Related Commands

Command	Description
show spanning-tree mst	Show the MSTP information of an interface.
spanning-tree mst cost	Set path cost.
spanning-tree mst port-priority	Set port priority of different instances.

Platform Description -

spanning-tree pathcost method

This command is used to configure the path cost of a port. You can use the **no** option of the command to restore the default setting.

spanning-tree pathcost method { { **long** [**standard**] } | **short** }

no spanning-tree pathcost method

Parameter Description

Parameter	Description
long [**standard**]	Adopt the 802.1t standard to set path cost. The "standard" indicates to use the expression recommended by the standard to calculate the cost.
short	Adopt the 802.1d standard to set path cost.

Defaults The 802.1T standard is adopted to set path cost by default.

Command Mode Global configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

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

Platform Description -

spanning-tree portfast

This command is used to enable the portfast on an interface. You can use the **disabled** option of this command to disable the portfast feature on the interface.

spanning-tree portfast [**disabled**]

Parameter Description

Parameter	Description
disabled	Disable the portfast on an interface.

Defaults

Disabled

Command Mode

Interface configuration mode

Usage Guide

-

Configuration Examples

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

Related Commands

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

Platform Description

-

spanning-tree portfast bpdufilter default

This command is used to enable the BPDU filter function globally. You can use the **no** option of the command to disable the BPDU filter.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Parameter Description

Parameter	Description
-	-

Defaults

Disabled

Command Mode

Global configuration mode

Usage Guide

Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the interface. You can use the **show spanning-tree** command to display the configuration.

Configuration

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

Examples

Related Commands

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

Platform Description -

spanning-tree portfast bpduguard default

This command is used to enable the BPDU guard globally. You can use the **no** option of the command to disable the BPDU guard.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Parameter Description

Parameter	Description
-	-

Defaults Disabled

Command Mode Global configuration mode

Usage Guide Once the BPDU guard is enabled on the interface, you will enter the error-disabled status if the BPDU message is received at the interface. You can use the **show spanning**-tree command to display the configuration.

Configuration Examples

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

Related Commands

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

Platform Description -

spanning-tree portfast default

This command is used to enable the portfast feature on all interfaces globally. You can use the **no** option of the command to disable the portfast on all the interfaces globally.

spanning-tree portfast default

no spanning-tree portfast default

Parameter

Parameter	Description

Description

-	-

Defaults Disabled

Command Mode Global configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

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

Platform Description -

spanning-tree reset

This command is used to restore the **spanning-tree** configuration to default. This command does not have the **no** option.

spanning-tree reset

Parameter Description

Parameter	Description
-	-

Command Mode Global configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

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

Platform Description -

spanning-tree tc-guard

This command is used to enable **tc-guard** on the interface to prevent the spread of TC messages. You can use the **no** option of this command to disable **tc-guard** on the interface.

spanning-tree tc-guard

no spanning-tree tc-guard

Parameter Description

Parameter	Description
-	-

Defaults

Disabled

Command Mode

Interface configuration mode

Usage Guide

-

Configuration Examples

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

Related Commands

Command	Description
-	-

Platform Description

-

spanning-tree tc-protection

This command is used to enable **tc-protection** globally. You can use the **no** option of this command to disable **tc- protection** globally.

spanning-tree tc- protection

no spanning-tree tc- protection

Parameter Description

Parameter	Description
-	-

Defaults

Enabled

Command Mode

Global configuration mode

Usage Guide

-

Configuration Examples

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

Related Commands

Command	Description
-	-

Platform Description -

spanning-tree tc-protection tc-guard

This command is used to enable **tc-guard** globally to prevent the spread of TC messages. You can use the **no** option of this command to disable **tc-guard** globally.

spanning-tree tc- protection tc-guard

no spanning-tree tc- protection tc-guard

Parameter Description

Parameter	Description
-	-

Defaults Disabled

Command Mode Global configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

Command	Description
-	-

Platform Description -

spanning-tree tx-hold-count

This command is used to configure the TxHoldCount of the STP in the global configuration mode and the maximum number of the BPDU messages sent in one second. You can use the **no** option of the command to restore the default setting.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

Parameter Description

Parameter	Description
tx-hold-count	Set TxholdCount in the range from 1 to 10.

Defaults The default value is 3.

Command Mode Global configuration mode

Usage Guide -

Configuration Examples

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

Related Commands

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

Platform Description -

Protocol Frames Transparent Transmission Configuration Commands

bridge-frame forwarding protocol bpdu

Use the **bridge-frame forwarding protocol bpdu** command to enable transparent transmission of BPDU frames. Use the **no** form of this command to disable transparent transmission of BPDU frames.

bridge-frame forwarding protocol bpdu

no bridge-frame forwarding protocol bpdu

Parameter Description

Parameter	Description
-	-

Defaults Transparent transmission of BPDU frames is disabled on a device by default.

Command Modes Global configuration mode

Usage Guidelines -

Examples Example 1: Enable transparent transmission of BPDU frames on a device.

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

Example 2: Disable transparent transmission of BPDU frames on the device.

```
Ruijie(config)# no bridge-frame forwarding protocol bpdu
```

Related Commands

Command	Description
-	-

Platform Description -

bridge-frame forwarding protocol gvrp

Use the **bridge-frame forwarding protocol gvrp** command to enable transparent transmission of GVRP frames. Use the **no** form of this command to disable transparent transmission of GVRP frames.

bridge-frame forwarding protocol gvrp

no bridge-frame forwarding protocol gvrp

Parameter Description

Parameter	Description
-	-

Defaults Transparent transmission of GVRP frames is disabled on a device by default.

Command modes Global configuration mode

Usage Guidelines -

Examples Example 1: Enable transparent transmission of GVRP frames on a device.

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

Example 2: Disable transparent transmission of GVRP frames on a device.

```
Ruijie(config)# no bridge-frame forwarding protocol gvrp
```

Related Commands

Command	Description
-	-

Platform Description -

bridge-frame forwarding protocol 802.1x

Use the **bridge-frame forwarding protocol 802.1x** command to enable transparent transmission of 802.1X frames. Use the **no** form of this command to disable transparent transmission of 802.1X frames.

bridge-frame forwarding protocol 802.1x

no bridge-frame forwarding protocol 802.1x

Parameter Description

Parameter	Description
-	-

Defaults Transparent transmission of 802.1X frames is enabled on a device by default.

Command Modes Global configuration mode

Usage Guidelines -

Examples Example 1: Enable transparent transmission of 802.1X frames on a device.

```
Ruijie(config)# bridge-frame forwarding protocol 802.1x
```

Example 2: Disable transparent transmission of 802.1X frames on the device.

```
Ruijie(config)# no bridge-frame forwarding protocol 802.1x
```

Related Commands

Command	Description
-	-

Platform Description

-

GVRP Configuration Commands

clear gvrp statistics

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

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

Parameter Description

Parameter	Description
interface-id	Interface id

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

Use the **show gvrp statistics** to show the statistics.

Configuration Examples

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

Related Commands

Command	Description
show gvrp statistics	Show the GVRP statistics.

Platform Description

N/A

gvrp applicant state

Use this command to set the port advertising mode, which determines whether to allow sending the GVRP advertisement on the port. Use the **no** form of this command to restore it to the default setting.

gvrp applicant state { **normal** | **non-applicant** }

no gvrp applicant state

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Allow sending the GVRP advertisement on the port.

Command mode

Interface configuration mode.

Usage Guide

Use the **show gvrp configuration** to show the related configurations.

Configuration Examples

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

Related Commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

Platform Description

N/A

gvrp dynamic-vlan-creation

Use this command to control whether to allow creating the vlan dynamically. Use the no form of this command to restore it to the default setting.

gvrp dynamic-vlan-creation enable

no gvrp dynamic-vlan-creation enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Creating the vlan dynamically is not allowed.

Command mode

Global configuration mode.

Usage Guide

Use the **show gvrp configuration** to show the related configurations.

Configuration Examples

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

Related Commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

Platform Description

N/A

gvrp enable

Use this command to enable the GVRP function. Use the **no** form of this command to restore it to the default setting.

gvrp enable

no gvrp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command mode Global configuration mode.

Usage Guide Use the **show gvrp configuration** to show the related configurations.

Configuration Examples

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

Related Commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

Platform Description N/A

gvrp registration mode

Use this command to set the registration mode to control whether to allow creating/registering/canceling the vlan dynamically on the port. Use the **no** form of this command to restore it to the default setting.

gvrp registration mode { **normal** | **disabled** }

no gvrp registration mode

Parameter Description

Parameter	Description
N/A	N/A

Defaults Creating/registering/canceling the vlan dynamically is allowed.

Command mode Interface configuration mode.

Usage Guide

Use the **show gvrp configuration** to show the related configurations.

Configuration Examples

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

Related Commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

Platform Description

N/A

gvrp timer

Use this command to set the GVRP timer. Use the **no** form of this command to restore it to the default setting.

gvrp timer { **join** | **leave** | **leaveall** } *timer_value*

no gvrp timer

Parameter Description

Parameter	Description
join *timer_value*	Control the maximum delay before sending the advertisement on the port. The actual sending interval is in the range of 0 to the maximum delay.
leave *timer_value*	Control the waiting time before removing the VLAN from the port with the Leave Message received. If the Join Message is received again within this time range, the port-VLAN relation still exists and the timer becomes invalid. If no Join Message is received on the port, the port status will be the Empty and removed from the VLAN member list.
leaveall *timer_value*	Control the minimum interval of sending the LeaveAll Message on the port. If the LeaveAll Message is received before the timer expires, the timer re-counts. If the timer expires, send the LeaveAll Message on the port and also send this Message to the port, so that the Leave timer begins counting. The actual sending interval ranges from leaveall to leaveall+join.

Defaults

Join timer: 200 ms;
Leave timer: 600 ms;
Leaveall timer: 10,000 ms.

Command mode

Global configuration mode.

Usage Guide

Use the **show gvrp configuration** to show the related configurations.

Configuration Examples

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

Related Commands

Command	Description
show gvrp configuration	Show the GVRP configurations.

Platform Description

N/A

show gvrp configuration

Use this command to show the GVRP configurations.

show gvrp configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

Use the **show gvrp configuration** to show the related configurations.

Configuration Examples

```
Ruijie# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
Join Timers(ms):600
Join Timers(ms):10000
Port based GVRP Configuration:
Port:GigabitEthernet 3/1 app mode:normal reg mode:normal
Port:GigabitEthernet 3/2 app mode:normal reg mode:normal
Port:GigabitEthernet 3/3 app mode:normal reg mode:normal
Port:GigabitEthernet 3/4 app mode:normal reg mode:normal
Port:GigabitEthernet 3/5 app mode:normal reg mode:normal
Port:GigabitEthernet 3/6 app mode:normal reg mode:normal
Port:GigabitEthernet 3/7 app mode:normal reg mode:normal
Port:GigabitEthernet 3/8 app mode:normal reg mode:normal
```

```
Port:GigabitEthernet 3/9 app mode:normal reg mode:normal
Port:GigabitEthernet 3/10 app mode:normal reg
mode:normal
Port:GigabitEthernet 3/11 app mode:normal reg
mode:normal
Port:GigabitEthernet 3/12 app mode:normal reg
mode:normal
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show gvrp statistics

Use this command to show the GVRP statistics of one interface or all interfaces.

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

Parameter Description

Parameter	Description
interface-id	Interface id.

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

Use the **show gvrp statistics** to show the statistics of one interface or all interfaces.

Configuration Examples

```
Ruijie# show gvrp statistics gigabitethernet 1/1
Interface      GigabitEthernet 3/1
RecValidGvrpPdu        0
RecInvalidGvrpPdu      0
RecJoinEmpty   0
RecJoinIn      0
RecEmpty       0
RecLeaveEmpty   0
RecLeaveIn     0
RecLeaveAll     0
SentGvrpPdu     0
SentJoinEmpty   0
SentJoinIn     0
```

```
SentEmpty      0
SentLeaveEmpty  0
SentLeaveIn    0
SentLeaveAll    0
JoinIndicated   0
LeaveIndicated  0
JoinPropagated  0
LeavePropagated  0
```

Related Commands

Command	Description
clear gvrp statistics	Clear the statistics of one interface or all interfaces.

Platform Description

N/A

show gvrp status

Use this command to show the GVRP status.

show gvrp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

Use the **show gvrp status** command to show the GVRP status.

Configuration Examples

```
Ruijie# show gvrp status
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

LLDP Configuration Commands

civic-location

Configure common LLDP address information. Use **no** form of this command to delete the address information.

{ **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 {**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 characters. China: 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

Default -

Command mode LLDP Civic Address configuration mode

Usage guidelines Enter the LLDP Civic Address configuration mode and configure common LLDP address information according to the following commands: **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** or **additional-code**). Note that the first key word of the command is not **civic-location**.

Examples Configure the information of LLDP Civic Address (ID: 1): country: CH; city: Fuzhou

```
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** }	Show the LLDP Civic Address information.

Platform description

clear lldp statistics

Clear LLDP statistics

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

Parameter description

Parameter	Description
interface-name	Interface name

Default -

Command mode Privileged EXEC mode

Usage guidelines **interface** parameter: clear the LLDP statistics of the specified interface.

Examples Clear 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
-	-

Platform description

clear lldp table

Clear LLDP neighbor information.

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

Parameter description

Parameter	Description
interface-name	Interface name

Default -

Command mode Privilege mode

Usage guidelines If the **interface** parameter is specified, clear the LLDP neighbor information of the specified interface. If the **interface** parameter is not specified, clear the LLDP neighbor information of all interfaces.

Examples Clear the LLDP neighbor information of 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**
-	-

Platform description

device-type

Configure device type information. Use **no** form of this command to delete the device type information.

device-type *device-type*

no device-type

Parameter description

Parameter	**Description**
device-type	Device type, Value range: 0-2 **0** indicates the device type is DHCP Server. **1** indicates the device type is Switch. **2** indicates the device type is LLDP MED terminal.

Default 1

Command mode LLDP Civic Address configuration mode

Usage guidelines Enter the LLDP Civic Address configuration mode and configure the device type in the common LLDP address information.

Examples Configure the information of lldp Civic Address (ID: 1): device type: 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** }	Show the LLDP Civic Address information.

Platform description

lldp enable

Enable the LLDP globally or on the interface. Use **no** form of this command to disable LLDP globally or on the interface.

lldp enable

no lldp enable

Parameter description

Parameter	Description
-	-

Default

Enabled.

Command mode

Global (or interface) configuration mode

Usage guidelines

LLDP takes effect on an interface only when LLDP is enabled globally.

Examples

Disable LLDP globally and on the interface:

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

Related commands

Command	Description
show lldp status	Display LLDP status information

Platform description

lldp encapsulation snap

Configure the encapsulation format of LLDP packets. By default, Ethernet II encapsulation is used.

lldp encapsulation snap

no lldp encapsulation snap

Parameter description

Parameter	Description
-	-

Default

By default, Ethernet II encapsulation format is used.

Command mode

Interface configuration mode.

Usage guidelines

Caution

To guarantee the normal communication between local device and neighbor device, the same LLDP packet encapsulation format must be used.

Examples

Configure LLDP packet encapsulation format to SNAP:

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
```

Related commands

Command	Description
show lldp status	Display LLDP status information.

Platform description

lldp error-detect

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.

lldp error-detect

no lldp error-detect

Parameter description

Parameter	Description
-	-

Default

LLDP error detection is enabled by default.

Command mode

Interface configuration mode.

Usage guidelines

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.

Examples

Configure LLDP error detection:

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

Related commands

Command	Description
show interface status	Display LLDP status information.

Platform description

lldp fast-count

When a new neighbor is found or the LLDP work mode is disabled or shifts into the TxRx or Tx mode, enable the fast sending mechanism to make the neighbor device learn the local device information as soon as possible. The fast sending mechanism shortens the sending cycle of LLDP packets to 1s. The device will continuously send a certain number of LLDP packets and restore its normal sending cycle.

lldp fast-count *value*

no lldp fast-count

Parameter description

Parameter	Description
value	The number of LLDP packets that the device fast sends, Default: 3, Configurable range: 1-10.

Default 3

Command mode Global configuration mode

Usage guidelines -

Examples

Configure the number of LLDP packets that the device fast sends to 5.

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

Related commands

Command	Description
show interface status	Show the LLDP status information.

Platform

description

lldp hold-multiplier

Configure the TTL multiplier. Use **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. Default: 4; configurable range: 2-10.

Default

The default multiplier is 4.

Command mode

Global configuration mode.

Usage guidelines

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.

Examples

Configure TTL multiplier to 5.

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

Related commands

Command	Description
show lldp status	Display LLDP status information.

Platform description

lldp location civic-location identifier

Enter the LLDP Civic Address configuration mode and create common address information of a network connection device. Use **no** form of this command to delete the LLDP Civic Address information.

lldp location civic-location identifier *id*

no lldp location civic-location identifier *id*

Parameter description

Parameter	Description
id	ID of the common address information of the network device. Range:

	1-1024.

Default

-

Command mode

Global configuration mode

Usage guidelines

Use this command to enter the LLDP Civic Address configuration mode.

Examples

Configure the Civic Address information of LLDP MED-TLV. ID: 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** }	Show the LLDP Civic Address information.

Platform description

lldp location elin identifier

Configure the encapsulated urgent phone number of Location Identification TLV. Use **no** form of this command to delete the urgent phone number information.

lldp location elin identifier *id* **elin-location** *tel-number*

no lldp location elin identifier *id*

Parameter description

Parameter	Description
id	ID of the urgent phone number information. Range: 1-1024.
tel-number	Urgent phone number. Range: 10-25 characters.

Default

-

Command mode

Global configuration mode

Usage guidelines

Use this command to configure urgent phone number information.

Examples

Create urgent phone number information.

```
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** }	Show the LLDP urgent phone number information.

Platform description

lldp management-address-tlv

Configure the management address advertised in LLDP packets. Use **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.

Default

By default, the management address advertised is the IPv4 address of the lowest-ID VLAN carried on the port.

Command mode

Interface configuration mode.

Usage guidelines

- 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.

Examples

Configure the management address advertised in LLDP packets to 192.168.1.1:

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
```

Related commands

Command	Description
show lldp local-information	Display LLDP local information

Platform description

lldp mode

Configure the LLDP operating mode. Use **no** form of this command to disable LLDP operating mode.

lldp mode {**rx** | **tx** | **txrx** }

no lldp mode

Parameter description

Parameter	Description
rx	Only sending LLDPDUs.
tx	Only receiving LLDPDUs.
txrx	Sending and receiving LLDPDUs

Default **txrx**

Command mode Interface configuration mode

Usage guidelines

- 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.

Examples Configure LLDP operating mode as tx on the interface:

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp mode tx
```

Related commands

Command	Description
show lldp status	Display LLDP status information

Platform description

lldp network-policy profile

Create an LLDP network policy and enter the LLDP network policy configuration mode. Use **no** form of this command to delete the LLDP network policy.

lldp network-policy profile *profile-num*

no lldp network-policy profile *profile-num*

Parameter description

Parameter	Description
profile-num	ID of the LLDP network-policy. Range: 1-1024.

Default

-

Command mode

Global configuration mode

Usage guidelines

Use this command to enter the LLDP network-policy configuration mode. Specify a policy ID before using this command.

After entering the LLDP network-policy configuration mode, run the { **voice** | **voice-signaling** } **vlan** command to configure a specific network policy.

Examples

Create an LLDP network-policy. ID: 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*]	Show the LLDP network policy.

Platform description

lldp notification remote-change enable

Configure LLDP Trap. Use **no** form of this command to disable LLDP Trap.

lldp notification remote-change enable

no lldp notification remote-change enable

Parameter description

Parameter	Description
-	-

Default

Disabled

Command mode

Interface configuration mode.

Usage guidelines

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.

Examples

Configure LLDP Trap:

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
```

Related commands

Command	Description
show lldp status	Display LLDP status information.

Platform description

lldp timer notification-interval

Configure an interval of sending LLDP Traps. Use **no** form of this command to restore to the default interval.

lldp timer notification-interval *seconds*

no lldp timer notification-interval

Parameter description

Parameter	Description
seconds	Configure the interval of sending LLDP Traps. Default: 5 seconds; configurable range: 5-3600 seconds.

Default

5 seconds

Command mode

Global configuration mode.

Usage guidelines

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.

Examples

Configure the interval of sending LLDP Traps to 10 seconds:

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

Related commands

Command	Description
show lldp status	Display LLDP status information.

Platform description

lldp timer reinit-delay

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

lldp timer reinit-delay *seconds*

no lldp timer reinit-delay

Parameter description

Parameter	Description
seconds	Port initialization delay. Configurable range: 1-10 seconds.

Default

2 seconds

Command mode

Global configuration mode.

Usage guidelines

To prevent LLDP from being initialized too frequently due to the frequent operating mode change, you can configure port initialization delay.

Examples

Configure LLDP port initialization delay to 3 seconds:

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

Related commands

Command	Description
show lldp status	Display LLDP status information.

Platform description

lldp timer tx-delay

Configure LLDP packet transmission delay. Use **no** form of this command to restore the transmission delay to the default setting.

lldp timer tx-delay *seconds*

no lldp timer tx-delay

Parameter description

Parameter	Description

seconds	LLDP packet transmission delay. Configurable range: 1-8192.

Default

2 seconds

Command mode

Global configuration mode.

Usage guidelines

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.

Examples

Configure LLDPDU transmission delay to 3 seconds:

```
Ruijie# configure terminal
Ruijie(config)#lldp timer tx-delay 3
```

Related commands

Command	Description
show lldp status	Display LLDP status information.

Platform description

lldp timer tx-interval

Configure the interval of sending the LLDP packets. Use **no** form of this command to restore the interval to the default setting.

lldp timer tx-interval *seconds*

no lldp timer tx-interval

Parameter description

Parameter	Description
seconds	Interval of sending the LLDP packets. Configurable range: 5-32768.

Default

30 seconds

Command mode

Global configuration mode.

Usage guidelines

-

Examples

Configure the interval of sending the LLDP packets to 10 seconds:

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

Related commands

Command	**Description**
show lldp status	Display LLDP status information.

Platform description

lldp tlv-enable

Configure the types of advertisable TLVs. Use **no** form of this command to cancel the advertising of specific TLV types.

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** | **capabilit**y | **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** | **capabilit**y | **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	Normal address information about the network device in location identification TLVs.
elin	Telephone numbers for urgencies in location identification TLVs
id	ID configured for the policy
network-policy	Network Policy TLV
profile-num	Network Policy ID
power-over-ethernet	Extended Power-via-MDI TLV

Default

By default, all TLVs other than Location Identification TLV can be advertised on the interface.

Command mode

Interface configuration mode.

Usage guidelines

- When configuring basic management TLVs, IEEE 802.1 organizationally specific TLVs and IEEE 802.3 organizationally specific TLVs, if the "**all**" parameter is specified, all corresponding optional TLVs will be advertised. When configuring LLDP-MED TLVs, if the "**all**" parameter is specified, all LLDP-MED TLVs other than Location Identification TLV will be advertised.
- When configuring LLDP-MED TLVs, the LLDP-MED Capability TLV shall be configured as advertisable in order to further configure other LLDP-MED TLVs as advertisable.
- In order not to advertise LLDP-MED Capability TLV, other LLDP-MED TLVs shall be configured as non-advertisable, so that LLDP-MED TLVs are not advertised.

Examples

Configure to advertise all IEEE 802.1 organizationally specific TLVs:

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable dot1-tlv all
```

Apply the LLDP network policy to the interface 0/1.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv network-policy profile 1
```

Apply the LLDP Civic Address configuration information (ID=1) to the interface 0/1.

```
Ruijie#config
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv location civic-location
```

```
identifier 1
```

Apply the emergency telephone number information (ID=1) to the interface 0/1.

```
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	Display the attributes of advertisable TLVs

Platform description

{voice | voice-signaling} vlan

Configure an LLDP network-policy. Use **no** form of this command to delete the policy application type.

{ **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	Specify the voice application type.
voice-signaling	Specify the voice-signaling application type.
vlan-id	(Optional) Specify the VLAN ID of voice flows. Range: 1-4094.
cos	(Optional) Class of service
cvalue	(Optional) Configure the COS value of voice flows. Range: 0-7. Default: 5.
dscp	(Optional) differentiated services code point
dvalue	(Optional) Configure the DSCP value of voice flows. Range: 0-63. Default: 46.
dot1p	(Optional) Configure 802.1p priority tagging. The TAG frame only contains user_priority. VLAN ID: 0.
none	(Optional) Indicates no network-policy will be delivered. VoIP decides the network policy based on VoIP configuration.
untagged	(Optional) Indicate VoIP sends untagged frames in the voice VLAN. The VLAN ID and COS values are ignored.

Default

-

Command mode

LLDP network-policy configuration mode

Usage guidelines

Enter the LLDP network-policy configuration mode and configure an LLDP network policy.

voice indicates the voice data type. **voice-signaling** indicates the voice signaling type.

Examples Configure the lldp network-policy (profile-num: 1): voice application type; ID: untagged; voice-signaling application type; VLAN ID: 3; COS: 4; DSCP: 6.

```
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*]	Show the LLDP network-policy.

Platform description

show lldp local-information

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

Default -

Command mode Privileged EXEC mode

Usage guidelines

- **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.

Examples Display 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                 : speed(100)/duplex(Half)
  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**
-	-

Platform description

show lldp location

Show the common LLDP address information or urgent phone number information of the local device.

show lldp location { **civic-location | elin** } { **identifier** *id* **| interface** *interface-name* **| static** }

Parameter description

Parameter	Description
civic-location	Indicates the common address information of the encapsulated network connectivity device.
elin	Indicates the encapsulated urgent phone number information.
identifier	Show the address information or urgent phone number information configured by a user.
id	Specify the policy ID configured by a user.
interface	Show the address information or urgent phone number information of an interface.
interface-name	Specify the name of an interface.
static	Show the address information or urgent phone number information configured by all users.

Default

-

Command mode

Privilege mode

Usage guidelines

- If a policy ID is specified, show the specific address information or urgent phone number information.
- If an interface name is specified, show the address information or urgent phone number information of the interface.
- If no parameter is specified, show all address information or urgent phone number information.

Examples

Show all address information:

```
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
--------------------------
```

Show all urgent phone number information.

```
Ruijie# show lldp location elin static
Elin location information
--------------------------
Identifier :                    t
Elin          :                     iiiiiiiii
Ports                        :    Gi1/0/3
--------------------------
```

Related commands

Command	Description
-	-

Platform description

show lldp neighbors

Show the LLDP information of neighbor devices.

show lldp neighbors [**interface** *interface-name*] [**detail**]

Parameter description

Parameter	Description
interface-name	Interface name
detail	Show all information of neighbor devices.

Default

-

Command mode

Privilege mode

Usage guidelines

- If the **detail** parameter is not specified, show the abstract information of neighbor devices.
- If the **detail** parameter is specified, show the detailed information of neighbor devices.
- If the **interface** parameter is specified, show the neighbor information received by the interface.

Examples

Show the neighbor information received by all interfaces.

```
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              :
```

Run the show lldp neighbors command to show the information description table.

Field	Description
Neighbor index	Neighbor index
Device type	Neighbor device type
Update time	The latest update time of neighbor information
Aging time	The aging time of neighbor information, that is, the number of seconds that will elapse before the neighbor information is deleted.
Chassis ID type	Chassis ID type
Chassis ID	Chassis ID is used to identify a device. MAC addresses are usually used as Chassis IDs.
System name	System name
System description	The description of the system, including hardware/software versions and operational system information.
System capabilities supported	Functions supported by the system
System capabilities enabled	Functions used by the system
Management address subtype	Management address type
Management address	Management address
Interface numbering subtype	Management address interface type
Interface number	Management address interface ID
Object identifier	Management address object ID
Device class	Med device types: Network connectivity device and terminal device. Network connectivity device Class I: common terminal devices Class II: media terminal devices. The devices have the capabilities of Class I and support media flows. Class III: communication terminal devices. The devices have the capabilities of Class I and Class II and support IP communication.
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Manufacturer name

Asset tracking identifier	Asset tracking ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID	Port and protocol VLAN ID
PPVID Supported	Whether to support port protocol VLAN
PPVID Enabled	Whether to enable the port protocol VLAN
VLAN name of VLAN 1	The name of VLAN 1
Protocol Identity	Protocol ID
Auto-negotiation supported	Whether to support auto-negotiation
Auto-negotiation enabled	Whether to enable the auto-negotiation
PMD auto-negotiation advertised	Port auto-negotiation advertisement capability
Operational MAU type	Port auto-negotiation speed and duplex status
PoE support	Whether to support PoE
Link aggregation supported	Whether to support link aggregation
Link aggregation enabled	Whether to enable link aggregation
Aggregation port ID	Link aggregation port ID
Maximum frame Size	The maximum frame size supported by the port.
Power-via-MDI device type	Device types, including: Power source equipment (PSE) Powered device (PD)
Power-via-MDI power source	Power supply type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Power supplied by the port.

Related commands

Command	**Description**
-	-

Platform description

show lldp network-policy profile

Show the LLDP network-policy information of the local device.

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

Parameter description

Parameter	**Description**
profile-num	ID of the network-policy. Range: 1-1024.

Default -

Command mode

Privilege mode

Usage guidelines

If a policy ID is specified, show the specific network-policy information.

If no parameter is specified, show all network-policy information.

Examples

Show all network-policy information.

```
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
-	-

Platform description

show lldp statistics

Display LLDP statistics.

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

Parameter description

Parameter	Description
interface-name	Interface name

Default

-

Command mode

Privileged EXEC mode

Usage guidelines

- **global** parameter: display the global LLDP statistics.
- **Interface** parameter: display the LLDP statistics of the specified interface.

Examples

Display 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
-	-

Platform description

show lldp status

Display LLDP status information.

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

Parameter description

Parameter	Description
interface-name	Interface name

Default

-

Command mode

Privileged EXEC mode

Usage guidelines

interface parameter: display the LLDP status information of the specified interface.

Examples

Display 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 statusCommand 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
-	-

Platform description

show lldp tlv-config

Display the advertisable TLV configuration of a port.

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

Parameter description

Parameter	Description
interface-name	Interface name

Default -

Command mode Privileged EXEC mode

Usage guidelines **Interface** parameter: display the LLDP TLV configuration of the specified interface.

Examples Display 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**
-	-

Platform description

QinQ Configuration Commands

dot1q outer-vid *vid* register inner-vid *v_list*

Use this command to configure the add policy list of outer vid based on protocol on tunnel port.

dot1q outer-vid *vid* **register inner-vid** *v_list*

no dot1q outer-vid *vid* **register inner-vid** *v_list*

Parameter description

Parameter	Description
v_list	Inner vlan id list
vid	Outer vlan id list
no	Remove the settings.

Default configuration

N/A.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring vid in the tag of input message as 4-22,adding the vid in the tag as 3:

```
Ruijie#configure
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport mode dot1q-tunnel
Ruijie(config-if)#dot1q outer-vid 3 register inner-vid 4-22
Ruijie(config-if)#end
```

Related commands

Command	Description
show registration-table [**interface** *intf-id*]	

Platform description

dot1q relay-vid *vid* translate local-vid *v-list*

Use this command to configure the modify policy list of outer vid based on protocol on access, trunk and hybrid port.

dot1q relay-vid *vid* **translate local-vid** *v-list*

no dot1q relay-vid *vid* **translate local-vid** *v-list*

Parameter description

Parameter	Description
v_list	Outer vlan list of input message
vid	Modified outer vlan id list
no	Remove the settings.

Default configuration

Null policy list.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring vid in the outer tag of input message as 10-20,modifying the vid as 100:

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode access
Ruijie(config-if)# dot1q relay-vid 100 translate local-vid 10-20
Ruijie(config-if)# end
```

Related commands

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

Platform description

dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

Use this command to map the priority from the outer tag to the inner tag for the packets on the interface.

dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

no dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

Parameter description

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

Default configuration

N/A.

Command mode

Interface configuration mode.

Usage guideline

N/A.

Examples

Here is an example of configuring the priority mapping from the outer tag to the inner tag:

```
ruijie# configure
ruijie(config)# interface gigabitEthernet 0/2
ruijie(config-if)# dot1q-tunnel cos 3 remark-cos 5
ruijie(config-if)# end
```

Related commands

Command	Description
show interface intf-name remark	

Platform description

frame-tag tpid

Use this command to set the manufacturer tpid.

frame-tag tpid *tpid*

no frame-tag tpid

Parameter description

Parameter	Description
no	Remove the setting.
tpid	manufacturer ID

Command mode

Interface configuration mode.

Examples

```
Ruijie(config)# interface g0/3
Ruijie(config-if)# frame-tag tpid 0x9100
Ruijie(config-if)# end
Ruijie# show frame-tag tpid
Port    tpid
------  ---------
Gi0/3     0x9100
```

Related commands

Command	Description
show frame-tag tpid	

Platform description

inner-priority-trust enable

Use this command to copy the priority of the inner tag to the outer tag of the packets on the interface.

inner-priority-trust enable

no inner-priority-trust enable

Parameter description

Parameter	Description
no	Remove the settings.

Command mode

Interface configuration mode.

Examples

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

Related commands

Command	Description
show inner-priority-trust	

Platform description

l2protocol-tunnel

Use this command to set the dot1q-tunnel port to receive L2 protocol message.

l2protocol-tunnel {stp | gvrp}

no l2protocol-tunnel {stp | gvrp}

Parameter description

Parameter	Description
stp	Receive stp message.
gvrp	Receive gvrp message.
no	Remove the settings.

Command mode

Global configuration mode.

Examples

Here is an example of enabling the function of receiving L2 protocol gvrp and stp:

```
Ruijie#configure
Ruijie(config)# l2protocol-tunnel stp
Ruijie(config)# l2protocol-tunnel gvrp
Ruijie(config)#end
```

Related commands

Command	Description
show l2protocol-tunnel { gvrp | stp }	

Platform description

l2protocol-tunnel *proto-type* enable

Use this command to enable transparent transmission of L2 protocol message.

l2protocol-tunnel {stp | gvrp} enable

no l2protocol-tunnel {stp | gvrp} enable

Parameter description

Parameter	Description
stp	Transparently transmit stp message.
gvrp	Transparently transmit gvrp message.
no	Remove the settings.

Command mode

Intereface configuration mode.

Examples

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

```
Ruijie#configure
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# l2protocol-tunnel gvrp enable
Ruijie(config-if)#end
```

Related commands

Command	Description
show l2protocol-tunnel {gvrp|stp}	

Platform description

l2protocol-tunnel proto-type tunnel-dmac *mac-address*

Use this command to set the MAC address for the transparent transmission of the corresponding protocol messages.

l2protocol-tunnel { stp|gvrp } tunnel-dmac *mac-address*

no l2protocol-tunnel { stp|gvrp } tunnel-dmac *mac-address*

Parameter description

Parameter	Description
stp	Set the STP transparent transmission address.
gvrp	Set the GVRP transparent transmission address.
mac-address	Transparent transmission address to be configured.
no	Restore the transparent transmission address to the default value. By default, the first three bytes of the transparent transmission address are 01d0f8, and the latest three bytes are (stp: 000005; grip: 000006)

Command mode

Global configuration mode.

Examples

Here is an example of setting the MAC address for the L2-protocol transparent transmission function：

```
Ruijie(config-if)# l2protocol-tunnel gvrp tunnel-dmac 011AA9
000005
Ruijie(config-if)#end
```

Related commands

Command	Description
show l2protocol-tunnel {gvrp|stp}	

Platform description

mac-address-mapping *index-id* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*

Use this command to copy the MAC address dynamically-learned from the source VLAN to the destination VLAN.

mac-address-mapping *index-id* **source-vlan** *src-vlan-id* **destination-vlan** *dst-vlan-list*

no mac-address-mapping *index-id* **source-vlan** *src-vlan-id* **destination-vlan** *dst-vlan-list*

Parameter description

Parameter	Description
no	Cancel to copy the MAC address dynamically-learned from the source VLAN to the destination VLAN.
index-id	MAC address copy policy ID.
src-vlan-list	The source VLAN list of the MAC address copy policy.
dst-vlan-list	The destination VLAN list of the MAC address copy policy.

Command mode

Interface configuration mode.

Examples

```
ruijie#configure
ruijie(config)# interface gigabitEthernet 0/2
ruijie(config-if)# mac-address-mapping 1 source-vlan 1-3
destination-vlan 5
ruijie(config-if)#end
```

Related commands

Command	Description
show interface mac-address-mapping x	

Platform description

switchport dot1q-tunnel allowed vlan

Use this command to configure the allowed VLAN of dot1q-tunnel.

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

switchport dot1q-tunnel allowed vlan *remove v_list*

no switchport dot1q-tunnel allowed vlan

Parameter description

Parameter	Description
add	Add the allowed vlan.
tagged	Tag-carried.
untagged	Not tag-carried.
v_list	vlan id list.
no	Remove the settings.

Default configuration

Allowed vlan 1,untagged.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring vlan 3-6 of dot1q-tunnel port as allowed VLAN and outputting the frame with tag:

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport dot1q-tunnel allowed vlan tagged 3-6
Ruijie(config)#end
```

Related commands

Command	Description
show interface dot1q-tunnel	

Platform description

switchport dot1q-tunnel native vlan

Use this command to configure the default vlan id of dot1q-tunnel.

switchport dot1q-tunnel native vlan *vid*

no switchport dot1q-tunnel native vlan

Parameter description

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

Default configuration

Vlan 1

Command mode

Interface configuration mode.

Examples

Here is an example of configuring default vlan of dot1q-tunnel port as 8:

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if)#switchport dot1q-tunnel native vlan 8
Ruijie(config)#end
```

Related commands

Command	Description
show interface dot1q-tunnel	

Platform description

switchport mode dot1q-tunnel

Use this command to configure the interface as the dot1q-tunnel interface.

switchport mode dot1q-tunnel

no switchport mode

Parameter description

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

Default configuration

No dot1q-tunnel interface is configured.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring the interface as the dot1q-tunnel interface:

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

Related commands

Command	Description
show vlan	

Platform description

switchport mode uplink

Use this command to configure the interface as an uplink port.

switchport mode uplink

no switchport mode

Parameter description

Parameter	Description
no	Remove the settings.

Default configuration

No uplink port is configured.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring the interface as a uplink port.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode up-link
Ruijie(config)# end
```

Related commands

Command	Description
show vlan	

Platform description

traffic-redirect access-group *acl* outer-vlan

Use this command to configure the modify policy list of outer vid based on flow on access,trunk,hybrid port.

traffic-redirect access-group *acl* **outer-vlan** *vid* **in**

no traffic-redirect access-group *acl* **outer-vlan**

Parameter description

Parameter	Description
acl	Flow matching.
vid	Modified outer vid list
no	Remove the settings.

Default configuration

Null policy list.

Command mode

Interface configuration mode.

Examples

Here is an example of configuring outer vid of input message whose source address is 1.1.1.1 as 3:

```
Ruijie# configure
Ruijie(config)#ip access-list standard 2
Ruijie(config-std-nacl)# permit host 1.1.1.1
Ruijie(config-std-nacl)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
Ruijie(config-if)# end
```

Related commands

Command	Description
show traffic-redirect	

Platform description

traffic-redirect access-group *acl* nested-vlan

Use this command to configure vid add policy list based on flow on dot1q-tunne port.

traffic-redirect access-group *acl* **nested-vlan** *vid* **in**

no traffic-redirect access-group *acl* **nested –vlan**

Parameter description

Parameter	Description
acl	Flow matching.
vid	vid list to be added.
no	Remove the settings.

Default configuration

Null policy list.

Command mode

Interface configuration mode.

Examples

Here is an example of adding the vid of input message whose source address is 1.1.1.3 as 9:

```
Ruijie#configure
Ruijie(config)#ip access-list standard 20
Ruijie(config-std-nacl)#permit host 1.1.1.3
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode dot1q-tunnel
Ruijie(config-if)# traffic-redirect access-group 20 nested-vlan 10
in
Ruijie(config-if)# end
```

Related commands

Command	Description
show traffic-redirect	

Platform description

vlan-mapping-in vlan *src-vlan-list* remark *dest-vlan*

Use this command to configure the policy list of the VLAN mapping in the incoming direction on the access, trunk, hybrid, uplink port.

vlan-mapping-in vlan *src-vlan-list* **remark** *dest-vlan*

no vlan-mapping-in vlan *src-vlan-list* **remark** *dest-vlan*

Parameter description

Parameter	Description
src-vlan-list	Vid list of the input packets.
dest-vlan	Modified vid
no	Remove the settings.

Default configuration

Null policy list.

Command mode

Interface configuration mode.

Examples

Here is an example of modifying the vid of the input messages whose vids in the tag ranges from 3 to 7 as 4 and forwarding it:

```
Ruijie# configure
Ruijie(config)# vlan range 3-8
Ruijie(config-vlan-range)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# vlan-mapping-in vlan 3-7 remark 8
Ruijie(config-if)# end
```

Related commands

Command	Description
show interface[*intf-id*] **vlan-mapping**	

Platform description

vlan-mapping-out vlan *src-vlan* remark *dest-vlan*

Use this command to configure the policy list of the one-to-one VLAN mapping in the outgoing direction on the acess, trunk, hybrid, uplink port.

vlan-mapping-out vlan *src-vlan* **remark** *dest-vlan*

no vlan-mapping-out vlan *src-vlan* **remark** *dest-vlan*

Parameter description

Parameter	Description
src-vlan	Vid of the input packets
dest-vlan	The modified vid

no	Remove the settings.

Default configuration

Null policy list.

Command mode

Interface configuration mode.

Examples

Here is an example of modifying the vid of the incoming messages whose vid in the tag is 3 as 4 and forwarding it:

```
Ruijie# configure
Ruijie(config)# vlan range 3-4
Ruijie(config-vlan-range)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# vlan-mapping-out vlan 3 remark 4
Ruijie(config-if)# end
```

Related commands

Command	Description
show interface [*intf-id*] **vlan-mapping**	

Platform description

show dot1q-tunnel

Use this command to show whether dot1q-tunnel of interface is enabled or not.

show dot1q-tunnel [**interface** *intf-id*]

Parameter description

Parameter	Description
intf-id	The specified interface.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Examples

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

Platform description

show frame-tag tpid

Use this command to show the configuration of interface tpid.

show frame-tag tpid [**interface** <*intf-id*>]

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration

The tpid is not modified.

Command mode

Privileged EXEC mode.

Examples

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

Platform description

show inner-priority-trust

Use this command to show the priority copy configuration.

show inner-priority-trust

Parameter description

N/A.

Default configuration

Priority copy is disabled by default.

Command

Privileged EXEC mode.

mode

Examples

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

Platform description

show interface dot1q-tunnel

Use this command to show dot1q-tunnel configuration.

show interface *[intf-id]* **dot1q-tunnel**

Parameter description

Parameter	Description
intf-id	The specified interface.

Default configuration N/A.

Command mode Privileged EXEC mode.

Examples

```
Ruijie# show interface dot1q-tunnel
Interface: Gi0/3
Native vlan: 10
Allowed vlan list: 4-6,10,30-60
Tagged vlan list: 4,6,30-60
```

Platform description

show interface intf-name remark

Use this command to show the priority mapping configurations.

show interface intf-name remark

Parameter description

Parameter	Description
-	-

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Examples

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

Platform description

show interface mac-address-mapping

Use this command to show the mac address mapping configurations.

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

Parameter description

Parameter	Description
index-id	MAC address copy policy ID.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Examples

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

Platform description

show interface vlan-mapping

Use this command to show the VLAN mapping configurations.

show interface vlan-mapping

Parameter description

Parameter	Description
-	-

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Examples

```
ruijie# show interface vlan-mapping
Ports         Type    Status Destination-VID  Source-VID-list
------------  ------  -----  ---------------- ---------------
Gi0/1         in       active       5                3
Gi0/1         out      active       3                5
```

Platform description

show l2protocol-tunnel

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

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

Parameter description

Parameter	Description
gvrp	Show configuration of transparently transmitting gvrp protocol.
stp	Show configuration of transparently transmitting stp protocol.

Default configuration

N/A .

Command mode

Privileged EXEC mode.

Examples

```
Ruijie# show l2protocol-tunnel stp
L2protocol-tunnel: Stp Enable
Ruijie# show l2protocol-tunnel gvrp
L2protocol-tunnel: gvrp Disable
```

Platform description

show registration-table

Use this command to show vid add policy list of protocol-based dot1q-tunnel port.

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

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration

Null policy list.

Command mode

Privileged EXEC mode.

Examples

```
Ruijie# show registration-table
Ports      Type    Outer-VID  Inner-VID-list
---------   ------  ------- -----------------
Gi0/7        Add-outer  5          7-10,15,20-30
```

Platform description

show traffic-redirect

Use this command to show flow-based vid change or add policy list.

show traffic-redirect [interface *intf-id***]**

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration

Null policy list.

Command mode

Privileged EXEC mode.

Examples

```
Ruijie# show traffic-redirect
Ports           Type          VID   Match-filter
------------ ----------- ---- ------------
Gi0/3        Mod-outer    23   11
Gi0/3        Mod-outer    3    4
Gi0/3        Mod-outer    6    5
Gi0/3        Mod-inner    8    inner-to-8
Gi0/6        Mod-inner    9    100
Gi0/7        Nested-vid   13   nest-13
```

Platform description

show translation-table

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

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

Parameter description

Parameter	Description
intf-id	Specific Interface

Default configuration

Null policy list.

Command mode

Privileged EXEC mode.

Examples

```
Ruijie# show translation-table
Ports        Type       Relay-VID  Old-local  Local\inner-VID-list
------------ ---------- ---------- ---------- ------------------
Gi0/7        Inner-CVID 8          N/A        10-20
Gi0/7        Local-SVID 1001       N/A        30-60
Gi0/7        In+Out     8          20         50
```

Platform description

ERPS Configuration Commands

associate sub-ring

Use this command to associate the ethernet ring with its sub-rings.

associate sub-ring raps-vlan *vlan-list*

no associate sub-ring raps-vlan *vlan-list*

Parameter description

Parameter	Description
vlan-list	Sub-rings' R-APS VLAN.

Default

By default, Ethernet ring is not associated with its sub-rings.

Command mode

ERPS configuration mode.

Usage guidelines

1) You need to configure this command on all nodes of the Ethernet ring, so as to transmit its sub-ring's ERPS protocol packets in the Ethernet ring.
2) Configuring the association is mainly to make the sub-ring's protocol packets transmit in the Ethernet ring. Users can also adopt the configuration command provided by the VLAN module to configure elaborately the VLAN and the relation between ports and VLAN, so as to transmit the sub-ring's protocol packets in other Ethernet rings and not leak the packets to the user network.

Examples

The following example associates the Ethernet sub-ring with other Ethernet rings:

#Enter the privileged EXEC mode

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

# Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

# Enter the erps configu

ration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

#Add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Configure the Ethernet subring

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)#  ring-port west fastEthernet 0/3 east virtual-channel
Ruijie(config-if)# exit
```

# Associate the subring with other Ethernet rings.

```
Ruijie(config)# erps raps-vlan 4093
Ruijie(config-erps4093)#  associate sub-ring raps-vlan 100
```

Related commands

Command	Description
-	-

Platform description

debug erps

Use this command to turn on the ERPS debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug erps {packet | event | error}

undebug erps {packet | event | error}

Parameter description

Parameter	Description
packet	Debugging information of the transcieved packets.
event	Event and state information.
error	Error debugging information.

Default N/A

Command mode Privileged EXEC mode.

Usage guidelines N/A

Examples N/A

Related commands

Command	Description
-	-

Platform description

erps enable

Use this command to enable/disable the ERPS function in the global configuration mode.

erps enable

no erps enable

Parameter description

Parameter	Description
-	-

Default Disabled

Command mode Global configuration mode.

Usage guidelines The ERPS protocol of the specified ring will begin running truly only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled.

Examples

The following example enables the ERPS protocol globally:

# Enter the privileged EXEC mode

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

# Enable the ERPS function globally.

```
Ruijie(config)# erps enable
```

# Enter the ERPS configuration mode

```
Ruijie(config)# erps raps-vlan 4093
```

# Enable the ERPS function for the specified ring.

```
Ruijie(config-erps4093)#  state enable
```

Related commands

Command	Description
state enable	After entering the ERPS configuration mode of the specified ring, configure this command to enable the ERPS protocol of this specified ring.

Platform description

erps monitor link-state by oam

Use this command to configure the method of monitoring the ERPS link state.

erps monitor link-state by oam vlan vlan-id

no erps monitor link-state by oam

Parameter description

Parameter	Description
-	-

Default

By default, it adopts the directly monitoring the link physical state (up or down) rather than the oam method.

Command mode

Global configuration mode.

Usage guidelines

For the link state monitoring, use the method of directly monitoring the link physical state (up or down), also monitor the logic state (unidirectional fault, bidirectional fault or normal) of the link by the OAM. By default, the former is adopted. If the OAM method is used, the inefficient link state monitoring may cause the convergence time longer when the topology changes.

Examples

The following example configures the method of monitoring the link state.

# Enter the privileged EXEC mode.

```
Ruijie# configure terminal
```

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

# Configure the method of monitoring the link state.

```
Ruijie(config)# erps monitor link-state by oam vlan 100
```

Related commands

Command	Description
-	-

Platform description

erps raps-vlan

Use this command to configure the R-APS VLAN of Ethernet ring.

erps raps-vlan *vlan-id*

no erps raps-vlan *vlan-id*

Parameter description

Parameter	Description
vlan-id	R-APS VLAN ID

Default

No R-APS VLAN is configured.

Command mode

Global configuration mode.

Usage guidelines

- The R-APS VLAN must be the VLAN that is not used on the device. Cannot set the VLAN1 to the R-APS VLAN.
- The same Ethernet ring of different devices needs the same R-APS VLAN.
- If you want to transparently transmit the ERPS protocol packets on a device without the ERPS function configured, make sure that only the two ports connected to the Ethernet ring on this device allow the R-APSA VLAN packets corresponding to this ERPS ring passing through. Otherwise, the other VLAN packets may enter the R-APS VLAN through the transparent transmission, causing the shock to the ERPS ring.

Examples

# Enter the privileged EXEC mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

#Configure the R-APS VLAN globally.

```
Ruijie(config)# erps raps-vlan 4093
```

Related commands

Command	Description
-	-

Platform description

protected-instance

Use this command to configure the VLAN protected by the Ethernet ring to implement the load balance function.

protected-instance *instance-id-list*

no protected-instance

Parameter description

Parameter	Description
instance-id-list	Instance protected by this Ethernet ring. (The VLANs corresponding to these instances are the VLANs protected by the Ethernet ring.)

Default

By default, all VLANs are protected.

Command mode

EPRS configuration mode.

Usage guidelines

The protected VLAN consists of the R-APS VLAN of this Ethernet ring and the data VLAN protected by this Ethernet ring.

Examples

Suppose that the ERP1 and ERP2 are configured on the switch to implement the load balance. The R-APS VLAN of the ERPS1 is 100, the protected data VLAN is in the range of 1 to 99 and 101-2000, the R-APS VLAN of the ERPS2 is 4093, and the protected data VLAN is in the range of 2001 to 4092 and 4094. Configuration for the load balance is shown as below:

# Enter the privileged EXEC mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

# Configure the VLAN configured by the ERP1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 100, 1-99, 101-2000

Ruijie(config-mst)# exit

Ruijie(config)# erps raps-vlan 100

Ruijie(config-erps100)#protected-instance 1
```

# Configure the VLAN configured by the ERP2.

```
Ruijie(config)# spanning-tree mst configuration

Ruijie(config-mst)# instance 2 vlan 4093, 2001-4092, 4094

Ruijie(config-mst)# exit

Ruijie(config)# erps raps-vlan 4093

Ruijie(config-erps4093)#protected-instance 2
```

Related commands

Command	Description
-	-

Platform description

ring-port

Use this command to configure the ERPS ring.

ring-port west {*interface-name1* | **virtual-channel**} **east** {*interface-name2* | **virtual-channel**}

no ring-port

Parameter description

Parameter	Description
interface-name1	Name of the West port.
interface-name2	Name of the East port.

Default

No ERPS ring is configured.

Command mode

EPRS configuration mode.

Usage guidelines

1) After adding the port to the ERP ring, the trunk attribute of the port is not allowed to be modified any more.
2) If the ring port is configured on the **virtual-channel**, this ring will be considered as a sub-ring.
3) Ports running the ERPS do not participate in the STP computing. ERPS, RERP and REUP do not share the port.

Examples

The following example is for the ERPS ring.

# Enter the privileged EXEC mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

# Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

# Enter the ERPS configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

#Add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config-erps4093)#  ring-port west fastEthernet 0/1 east
fastEthernet 0/2
```

Related commands

Command	Description
state enable	Enable the ERPS protocol of the specified ring in the ERPS mode of the specified ring.
sub-ring associate raps-vlan *vlan-id*	Establish the association between the subring and other Ethernet rings in the subring ERPS configuration mode.

Platform description

rpl-port

Use this command to configure the RPL port and RPL owner.

rpl-port {west | east} [rpl-owner]

no rpl-port

Parameter description

Parameter	Description
-	-

Default

No RPL port and RPL owner are configured.

Command mode

EPRS configuration mode.

Usage guidelines

- Up to one RPL link and one RPL owner node are needed and configurable for each ring.
- The non-RPL owner node does not need to be configured with the PRL port. Please perform configuration on the port connected with the PRL link if you want to configure a PRL port.

Examples

The following example configures the RPL port and RPL owner.

# Enter the privileged EXEC mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

# Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

# Enter the ERPS configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Specify the port where the RPL link is and the RPL owner.

```
Ruijie(config-erps4093)#  rpl-port west rpl-owner
```

Related

Command	Description

commands

ring-port west {*interface-name1* | **virtual-channel**} **east** {*interface-name2* | **virtual-channel**}	Configure the specified ERP ring in the ERPS configuration mode of the specified ring.
state enable	Enable the ERPS protocol of the specified ring in the ERPS configuration mode of the specified ring.

Platform description

show erps

Use this command to show the parameters and states of the ERPS.

show erps [{global | raps_vlan *vlan-id* **[sub-ring] }]**

Parameter description

Parameter	Description
-	-

Default

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

The following example shows the use of this command.

```
Ruijie# show erps
ERPS Information
Global Status                  : Enabled
Link monitored by         : Not Oam
--------------------------------------------
R-APS VLAN                     : 4092
Ring Status                    : Enabled
West Port                      : Gi 0/5 (Blocking)
East Port                      : Gi 0/7 (Forwarding)
RPL Port                       : West Port
RPL Port Blocked VLAN     : All
RPL Owner                      : Enabled
Holdoff Time                   : 0 milliseconds
Guard Time                     : 500 milliseconds
WTR Time                       : 5 minutes
Current Ring State             : Idle
--------------------------------------------
R-APS VLAN                     : 4093
Ring Status                    : Enabled
West Port                      : Virtual Channel
East Port                      : Gi 0/10 (Forwarding)
RPL Port                       : None
RPL Port Blocked VLAN          : All
RPL Owner                      : Disabled
Holdoff Time                   : 0 milliseconds
Guard Time                     : 500 milliseconds
WTR Time                       : 5 minutes
Current Ring State             : Idle
--------------------------------------------
R-APS VLAN                     : 4094
Ring Status                    : Enabled
West Port                      : Virtual Channel
East Port                      : 12 (Forwarding)
RPL Port                       : None
RPL Port Blocked VLAN          : All
RPL Owner                      : Disabled
Holdoff Time                   : 0 milliseconds
Guard Time                     : 500 milliseconds
WTR Time                       : 5 minutes
Current Ring State             : Idle
```

```
Ruijie# show erps raps_vlan 4093 sub-ring
R-APS VLAN: 4093
Sub-Ring R-APS VLANs    TC Propagation State
-------------------     ---------------------
100                     Enable
200                     Enable
```

Related commands

Command	Description
-	-

Platform description

state enable

Use this command to enable/disable the specified R-APS ring.

state enable

no state enable

Parameter description

Parameter	Description
-	-

Default

Disabled

Command mode

EPRS configuration mode.

Usage guidelines

1) Only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled, the ERPS protocol of the specified ring will begin truly running.

Examples

The following example enables the specified ERPS ring:

#Enter the privileged EXEC mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

#Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

# Enter the ERPS configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

# Enable the ERPS function for the specified ring.

```
Ruijie(config-erps4093)#state enable
```

# Enable the global ERPS function.

```
Ruijie(config-erps4093)# exit
Ruijie(config)# erps enable
```

Related commands

Command	Description
erps enable	Enable the global ERPS protocol.

Platform description

sub-ring tc-propagation

Use this command to specify the devices corresponding to the crossing node on the crossing ring whether to send out the notification when the subring topology changes.

sub-ring tc_propagation enable

no sub-ring tc_propagation

Parameter description

Parameter	Description
-	-

Default

By default, the topology changing notification is not sent.

Command mode

EPRS configuration mode.

Usage guidelines

This command is just needed to be configured on the crossing nodes on the crossing ring.

Examples

The following example is configured when the subring topology changes.

# Enter the privileged EXEC mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

#Configure the link mode of the Ethernet ring port and the default VLAN.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
```

# Enter the ERPS configuration mode.

```
Ruijie(config)# erps raps-vlan 4093
```

# Add the ports that participate in the ERPS protocol computing to the Ethernet ring.

```
Ruijie(config-erps4093)#  ring-port west fastEthernet 0/1 east fastEthernet 0/2
```

#Configure the Ethernet subring.

```
Ruijie(config)# erps raps-vlan 100
Ruijie(config)# interface fastEthernet 0/3
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# exit
Ruijie(config)# erps raps-vlan 100
Ruijie(config-erps100)#  ring-port west fastEthernet 0/3 east virtual-channel
```

# Associate the subring with other Ethernet rings.

```
Ruijie(config-erps100)#  sub-ring associate raps-vlan 4093
```

# Enable the topology changing notification for the subring.

```
Ruijie(config-erps100)#  sub-ring tc-propagation enable
```

Related commands

Command	Description
-	-

Platform description

timer

Use this command to configure the timer of the ERPS protocol.

timer { holdoff-time *interval1* **| guard-time** *interval2* **| wtr-time** *interval3* **}**

no timer { holdoff-time | guard-time | wtr-time }

Parameter description

Parameter	Description
interval1	Value of the Holdoff timer in 100 milliseconds, the valid range is 0 to 100.
interval2	Value of the Guard timer in 10 milliseconds, the valid range is 1 to 200.
interval3	Value of the WTR in minute, the valid range is 5 to 12.

Default

Holdoff timer: 0.

Guard timer: 500 milliseconds.

WTP timer: 5 seconds.

Command mode

EPRS configuration mode.

Usage guidelines

- **Holdoff timer:** This timer is used to avoid the ERPS from topology switching continuously due to the link intermittent fault. With this timer configured, if the link fault is detected, the ERPS does not perform the topology switching immediately until the timer times out and the link fault is verified.
- **Guard timer:** This timer is used to prevent the device receiving the timed-out R-APS messages. When the device detects the recovery from failure of the link, it sends out the message of link recovery and starts up the Guard timer. Before the Guard times out, except for the flush packets indicating the subring topology change, other packets are discarded directly without being handled.
- **WTR(Wait-to-restore) timer:** This timer is only valid for the RPL owner device. It is mainly used to prevent the RPL owner making the erroneous judgment to the ring network status. When the RPL detects the fault recovery, it does not perform the topology switching immediately until the WTR times out and the Ethernet ring indeed recovers from the fault. If the ring network fault is checked again before the WTR times out, then the WTR timer will be canceled and topology switching will be not executed any longer.

Examples

The following example configures the timer of the ERPS protocol.

# Enter the privileged EXEC mode.

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
# Enter the ERPS configuration mode.
Ruijie(config)# erps raps-vlan 4093
```

# Configure the protocol timer.

```
Ruijie(config-erps4093)#  timer holdoff-time 10
Ruijie(config-erps4093)#  timer guard-time 10
Ruijie(config-erps4093)#  timer wtr-time 10
```

Related commands

Command	Description
-	-

Platform description

IP Address and Application Configuration Commands

1. IP Address Configuration Commands
2. IPv6 Configuration Commands
3. DHCP Configuration Commands
4. DHCPv6 Configuration Commands
5. DNS Configuration Commands
6. FTP Server Configuration Commands
7. FTP Client Configuration Commands
8. Network Connectivity Test Tool Configuration Commands
9. TCP Configuration Commands
10. IPv4 REF Configuration Commands

IP Address Configuration Commands

arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. The **no** form of this command deletes the static MAC address mapping.

arp *ip-address MAC-address type*

no arp *ip-address MAC-address type*

Parameter Description

Parameter	Description
ip-address	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
MAC-address	48-bit data link layer address
type	ARP encapsulation type. The keyword is arpa for the Ethernet interface.

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 is an example of setting an ARP static mapping record for a host in the Ethernet.

```
arp 1.1.1.1 4e54.3800.0002 arpa
```

Related Commands

Command	Description
clear arp-cache	Clear the ARP cache table

Platform Description N/A

arp anti-ip-attack

For the messages corresponds to the directly-connected route, if the switch does not learn the ARP that corresponds to the destination IP address, it is not able to forward the message in hardware, and it needs to send the message to the CPU to resolve the address(that is the ARP learning). Sending large number of this message to the CPU will influence the other tasks of the switch. To prevent the IP messages from attacking the CPU, a discarded entry is set to the hardware during the address resolution, so that all sequential messages with that destination IP address are not sent to the CPU. After the address resolution, the entry is updated to the forwarding status, so that the switch could forward the message with that destination IP address in hardware.

In general, during the ARP request ,if the switch CPU receives three destination IP address messages corresponding to the ARP entry, it is considered to be possible to attack the CPU and the switch sets the discarded entry to prevent the unknown unicast message from attacking the CPU. User could set the *num* parameter of this command to decide whether it attacks the CPU in specific network environment or disable this function. Use the **arp anti-ip-attack** command to set the parameter or disable this function. The **no** form of this command restores it to default value 3.

arp anti-ip-attack *num*

no arp anti-ip-attack

Parameter Description

Parameter	Description
num	The number of the IP message to trigger the ARP to set the discarded entry in the range of 0 to 100. 0 stands for disabling the arp anti-ip-attack function.

Defaults

By default, set the discarded entry after 3 unknown unicast messages are sent to the CPU.

Command Mode

Global configuration mode.

Usage Guide

The arp anti-ip-attack function needs to occupy the switch hardware routing resources when attacked by the unknown unicast message. If there are enough resources, the arp anti-ip-attack *num* could be smaller. If not, in order to preferential ensure the use of the normal routing, the *num* could be larger or disable this function.

Configuration Examples

The following configuration sets the IP message number that triggers to set the discarding entry as 5.

```
Ruijie(config)# arp anti-ip-attack 5
```

The following configuration disables the ARP anti-ip-attack function.

```
Ruijie(config)# arp anti-ip-attack 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface. The **no** form of this command disables this function on the interface.

arp gratuitous-send interval *seconds*

no arp gratuitous-send

Parameter Description

Parameter	Description
seconds	The time interval to send the free ARP request message in the range 1 to 3600 seconds

Defaults This function is not enabled on the interface to send the free ARP request regularly.

Command Mode Interface configuration mode.

Usage Guide If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

Configuration Examples The following configuration sets to send one free ARP request to SVI 1 per second.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# arp gratuitous-send interval 1
```

The following configuration stops sending the free ARP request to SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# no arp gratuitous-send
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. The **no** form of this command is used 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 for retrying the ARP request message in the range of 1 to 3,600 seconds, 1 second by default

Defaults The retry interval of the ARP request is 1 second.

Command Mode Global configuration mode.

Usage Guide The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

Configuration Examples The following configuration sets the retry interval of the ARP request as 30s.

```
arp retry interval 30
```

Related Commands

Command	Description
arp retry times *number*	Set the retry time of the ARP request message.

Platform Description N/A

arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. The **no** form of this command can be used to restore the default 5 times of the ARP retry 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 1 to100. When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent.

Defaults

If the ARP response message is not received, the ARP request message will be sent for 5 times, and then it will be timed out.

Command Mode

Global configuration mode.

Usage Guide

The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

Configuration Examples

The following configuration will set the local ARP request not to be retried.

```
arp retry times 1
```

The following configuration will set the local ARP request to be retried for one time.

```
arp retry times 2
```

Related Commands

Command	Description
arp retry interval *seconds*	Set the retry interval of the ARP request message.

Platform Description

N/A

arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache. The **no** form of this command restores it to the default configuration.

arp timeout *seconds*

no arp timeout

Parameter Description

Parameter	Description
seconds	The timeout ranging 0 to 2,147,483 seconds

Defaults The default timeout is 3,600 seconds.

Command Mode Interface configuration mode.

Usage Guide The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

Configuration Examples The following is an example of setting the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet port 0/1 to 120 seconds.

```
interface fastEthernet 0/1
arp timeout 120
```

Related Commands

Command	Description
clear arp-cache	Clear the ARP cache list.
show interface	Show the interface information

Platform Description N/A

arp unresolve

Use this command to configure the maximum number of the unresolved ARP entries. The **no** form of this command can restore the default value of 8,192**.**

arp unresolve *number*

no arp unresolve

Parameter Description

Parameter	Description
number	The maximum number of the unresolved ARP entries in the range of 1 to 8192. The default value is 8,192.

Defaults The ARP cache table can contain up to 8,192 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, this command can be used to limit the quantity of the unresolved entries.

Configuration Examples

The following configuration sets the maximum number of the unresolved items as 500.

```
arp unresolve 500Ruijie(config-interface-vfc)#bind mac-address
001d.0928.b62f
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table in privileged EXEC mode

clear arp-cache [**trusted**] [*ip* [*mask*]] | **interface** *interface-name*]

N/A

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command can be used to refresh an ARP cache table.

Caution

On a NFPP-based(Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two **clear arp** times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.

Configuration Examples

The following is an example of removing all dynamic ARP mapping records.

```
clear arp-cache
The following is an example of removing dynamic ARP table entry 1.1.1.1
clear arp-cache 1.1.1.1
```

The following is an example of removing dynamic ARP table entry on interface SVI1

```
clear arp-cache interface Vlan 1
```

Related Commands

Command	Description
arp	Add a static mapping record to the ARP cache table.

Platform Description

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 user mode.

clear ip route { *** |** *network* [*netmask*] }

Parameter Description

Parameter	Description
*	Remove 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 temporary communication failure in the entire network.

Configuration Examples The example below refreshes only the route of 192.168.12.0.

```
clear ip route 192.168.12.0
```

Related Commands

Command	Description
show ip route	Show the IP routing table.

Platform Description

ip-address

Use this command to configure the IP address of an interface. The **no** form of this command can be used 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, with 8 bits in one group in decimal format. Groups are separated by dots.
network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.
secondary	Indicates the secondary IP address that has been configured.
gateway ip-address	Configure the gateway address for the layer-2 switch, which is only supported on the layer-2 switches. No address is followed by the gateway when using the no form of this command.

Defaults No IP address is configured for the interface.

Command Mode N/A

Usage Guide Interface configuration mode.

The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value "1" are the network address. The IP address bits that correspond to value "0" are the host address. For example, the network mask of Class A IP address is "255.0.0.0". You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The RGOS software supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary IP addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses. The secondary IP address and the primary IP address must belong to the same network or different networks. Secondary IP addresses are often used in network construction. Typically, you can try to use secondary IP addresses in the following situations:

- A network hasn't enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured.

- Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet.
- Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces of a device.

In general, the layer-2 switch is configured a default gateway with the **ip default-gateway** command. Sometimes the layer-2 switch may be managed through the telnet, and the management IP and default gateway of the layer-2 switch needed to be modified. In this case, after configuring any one of the **ip address** and **ip default-gateway** command, the other cannot be configured any more due to the configuration change which causes failing to access this device through the network. So you need to use the keyword **gateway** in the **ip address** command to modify both the management IP and default gateway. The keyword **gateway** is not in the output of **show running config**, but in the output of **ip default-gate** command.

Configuration Examples

In the example below, the primary IP address is configured as 10.10.10.1, and the network mask is configured as 255.255.255.0.

```
ip address 10.10.10.1 255.255.255.0
```

In the example below, the default gateway is configured as 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	Show detailed information of the interface.

Platform Description

ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. The **no** form of this command is used to remove the broadcast address configuration.

ip broadcast-addresss *ip-address*

no ip broadcast-addresss

Parameter Description

Parameter	Description
ip-address	Broadcast address of IP network

Defaults The default IP broadcast address is 255.255.255.255.

Command Mode Interface configuration mode.

Usage Guide At present, the destination address of IP broadcast packet is all “1”, represented as 255.255.255.255. The RGOS software can generate broadcast packets with other IP addresses through definition, and can receive both all “1” and the broadcast packets defined by itself.

Configuration Examples The following is an example of setting 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

ip default-gateway

Use this command to configure the default gateway on the Layer2 switch. Use the **no** form of this command to remove the default gateway.

ip default-gateway

no ip default-gateway

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, no default gateway is configured.

Command Mode Global configuration mode.

Usage Guide The packets will be sent to the default gateway if the destination address is unknown. Use the **show ip redirects** command to view the default gateway.

Configuration The following is an example of setting the default gateway 192.168.1.1:

Examples

```
ip default-gateway 192.168.1.1
```

Related Commands

Command	Description
show ip redirects	Show the default gateway, which is supported on the Layer 2 switch only.

Platform Description

ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. The **no** form of this command is used to remove the configuration.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter Description

Parameter	Description
access-list-number	(Optional) Access list number ranging 1 to 199 and 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

Defaults Disabled.

Command Mode Interface configuration mode.

Usage Guide IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all “1”), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast.

If the **no ip directed-broadcast** command is configured on an interface, RGOS will discard the directed broadcast packets received from the directly connected network.

Configuration Examples

The following is an example of enabling forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device.

```
interface fastEthernet 0/1
ip directed-broadcast
```

Related Commands

Command	Description
N/A	N/A

Platform Description

ip mask-reply

Use this command to configure the RGOS software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. The **no** form of this command is used to prohibit from sending the ICMP mask response message.

ip mask-reply

no ip mask-reply

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, no ICMP mask response message is sent.

Command mode

Interface configuration mode.

Usage Guide

Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

Configuration Examples

The following is an example of setting the FastEthernet 0/1 interface of a device to respond the ICMP mask request message.

```
interface fastEthernet 0/1
ip mask-reply
```

Related Commands

Command	Description

Platform Description

ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. The **no** form of this command is used to restore it to the default configuration.

ip mtu *bytes*

no ip mtu

Parameter Description

Parameter	Description
bytes	Maximum transmission unit of IP packet ranging 68 to 1500 bytes

Defaults It is the same as the value configured in the interface command **mtu** by default.

Command Mode Interface configuration mode.

Usage Guide If an IP packet is larger than the IP MTU, the RGOS software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.

If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

Configuration Examples The following is an example of setting the IP MTU value of the fastEthernet 0/1 interface to 512 bytes.

```
interface fastEthernet 0/1
ip mtu 512
```

Related Commands

Command	Description
mtu	Set the MTU value of an interface.

Platform Description

ip proxy-arp

Use this command to enable ARP proxy function on the interface. The **no** form of this command disables ARP function.

ip proxy-arp

no ip proxy-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Interface configuration mode.

Usage Guide Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

Configuration Examples The following is an example of enabling ARP on FastEthernet port 0/1:

```
interface fastEthernet 0/1
ip proxy-arp
```

Related Commands

Command	Description
N/A	N/A

Platform Description

ip redirects

Use this command to allow the RGOS software to send an ICMP redirection message in the interface configuration mode. The **no** form of this command is used to disable the ICMP redirection function.

ip redirects

no ip redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Enabled.

Command Mode

Interface configuration mode.

Usage Guide

When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.

The RGOS software enables ICMP redirection by default

Configuration Examples

The following is an example of disabling ICMP redirection for the fastEthernet 0/1 interface.

```
interface fastEthernet 0/1
no ip redirects
```

Related Commands

Command	Description
N/A	N/A

Platform Description

ip source-route

Use this command to allow the RGOS software to process an IP packet with source route information in global configuration mode. The **no** form of this command is used to disable the source route information processing function.

ip source-route

no ip source-route

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Enabled.

Command Mode

Global configuration mode.

Usage Guide

RGOS supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded.

The RGOS software supports IP source route by default.

Configuration Examples

The following is an example of disabling the IP source route.

```
no ip source-route
```

Related Commands

Command	Description
N/A	N/A

Platform Description

ip unnumbered

Use this command to configure an unnumbered interface. After an interface is configured as unnumbered interface, it is allowed to run the IP protocol and can receive and send IP packets. The **no** form can be used to remove this configuration.

ip unnumbered *interface-type interface-number*

no ip unnumbered

Parameter Description

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

Defaults

N/A.

Command mode

Interface configuration mode.

Usage Guide

Unnumbered interface is an interface that has IP enabled on it 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:

- An Ethernet interface cannot be configured as an unnumbered interface.

- 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.
- 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.
- The network cannot be started using an unnumbered interface.

Configuration Examples

In the example below the local interface is configured as an unnumbered interface，and the associated interface is FastEthernet 0/1. An IP address must be configured for the associated interface.

```
ip unnumbered fastEthernet 0/1
```

Related Commands

Command	Description
show interface	Show detailed information of the interface.

Platform Description

ip unreachables

Use this command to allow the RGOS software to generate ICMP destination unreachable messages. The **no** form of this command disables this function.

ip unreachables

no ip unreachables

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Enabled.

Command Mode

Interface configuration mode.

Usage Guide

RGOS software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and cannot process the upper protocol of this message.

RGOS software will send ICMP host unreachable message to source data if it cannot forward a message due to no routing.

This command influences all ICMP destination unreachable messages.

Configuration Examples

The following example disables sending ICMP destination unreachable message on FastEthernet 0/1.

```
interface fastEthernet 0/1
no ip unreachables
```

Related Commands

Command	Description
N/A	N/A

Platform Description

show arp

Use this command to show the Address Resolution Protocol (ARP) cache table

show arp [*ip* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]

Parameter Description

Parameter	Description
ip	Show the ARP entry of the specified IP address.
ip mask	Show the ARP entries of the network segment included within the mask.
static	Show all the static ARP entries.
complete	Show all the resolved dynamic ARP entries.
incomplete	Show all the unresolved dynamic ARP entries.
mac-address	Show the ARP entry with the specified mac address.

Defaults

N/A

Command Mode

Any

Usage Guide

N/A

Configuration Examples

The following is the output result of the **show arp** command:

```
Ruijie# show arp
Total Numbers of Arp: 7
Protocol   Address              Age(min)   Hardware          Type
Interface
Internet  192.168.195.68   0        0013.20a5.7a5f  arpa   VLAN 1
Internet  192.168.195.67   0        001a.a0b5.378d  arpa   VLAN 1
Internet  192.168.195.65   0        0018.8b7b.713e  arpa   VLAN 1
Internet  192.168.195.64   0        0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.63   0        001a.a0b5.3990  arpa   VLAN 1
Internet  192.168.195.62   0        001a.a0b5.0b25  arpa   VLAN 1
Internet  192.168.195.5   --        00d0.f822.33b1  arpa   VLAN 1
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with “-”.
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses
Interface	Interface associated with the IP addresses

The following is the output result of show arp 192.168.195.68

```
Ruijie# show arp 192.168.195.68
Protocol  Address    Age(min)  Hardware       Type   Interface
Internet  192.168.195.68   1   0013.20a5.7a5f  arpa   VLAN 1
```

The following is the output result of **show arp** 192.168.195.0 255.255.255.0

```
Ruijie# show arp 192.168.195.0 255.255.255.0
Protocol  Address    Age(min)  Hardware   Type   Interface
Internet  192.168.195.64   0   0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.2    1   00d0.f8ff.f00e  arpa   VLAN 1
Internet  192.168.195.5   --   00d0.f822.33b1  arpa   VLAN 1
Internet  192.168.195.1    0   00d0.f8a6.5af7  arpa   VLAN 1
Internet  192.168.195.51   1   0018.8b82.8691  arpa   VLAN 1
```

The following is the output result of **show arp** 001a.a0b5.378d

```
Ruijie# show arp 001a.a0b5.378d
Protocol  Address  Age(min)  Hardware  Type   Interface
Internet  192.168.195.67   4   001a.a0b5.378d  arpa   VLAN 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

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.

Usage Guide N/A

Configuration Examples

The following is 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 detail

Use this command to show the details of the Address Resolution Protocol (ARP) cache table.

show arp detail [*interface-type interface-number* | *ip* [*mask*] | *mac-address* | **static | complete | incomplete**]

Parameter Description

Parameter	Description

interface-type interface-number	Show the ARP of the layer 2 port or the layer 3 interface.
ip	Show the ARP entry of the specified IP address.
ip mask	Show the ARP entries of the network segment included within the mask.
mac-address	Show the ARP entry of the specified MAC address.
static	Show all the static ARP entries.
completev	Show all the resolved dynamic ARP entries.
incomplete	Show all the unresolved dynamic ARP entries.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to show the ARP details, such as the ARP type (Dynamic, Static, Local, Trust), the information on the layer2 port.

Configuration Examples The following is the output result of the **show arp detail** command:

```
Ruijie# show arp detail
IP Address        MAC Address       Type       Age(min)
Interface  Port
20.1.1.1          000f.e200.0001    Static     --    --
--
20.1.1.1         000f.e200.0001    Static     --    Vl3
--
20.1.1.1         000f.e200.0001    Static     --    Vl3
Gi2/0/1
193.1.1.70       00e0.fe50.6503    Dynamic    1     Vl3
Gi2/0/1
192.168.0.1         0012.a990.2241      Dynamic      10
Gi2/0/3   Gi2/0/3
192.168.0.1      0012.a990.2241    Dynamic    20    Ag1
Ag1
192.168.0.1      0012.a990.2241    Dynamic    30    Vl2
Ag2
192.168.0.39     0012.a990.2241    Local      --    Vl3
--
192.168.0.39       0012.a990.2241      Local         --
Gi2/0/3   --
192.168.0.1      0012.a990.2241    Local      --    Vl3
--
192.168.0.1         0012.a990.2241      Local         --
Gi2/3/2   --
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
IP Address	IP address corresponding to the hardware address
MAC Address	hardware address corresponding to the IP address
Age (min)	Age of the ARP learning, in minutes
Port	Layer2 port associated with the ARP
Type	ARP type, includes the Static, Dynamic, Trust, Local.
Interface	Layer 3 interface associated with the IP addresses

Related Commands

Command	**Description**

Platform Description

show arp packet statistics

Use this command to show the statistics of ARP packets.

show arp packet statistics [*interface-name*]

Parameter Description

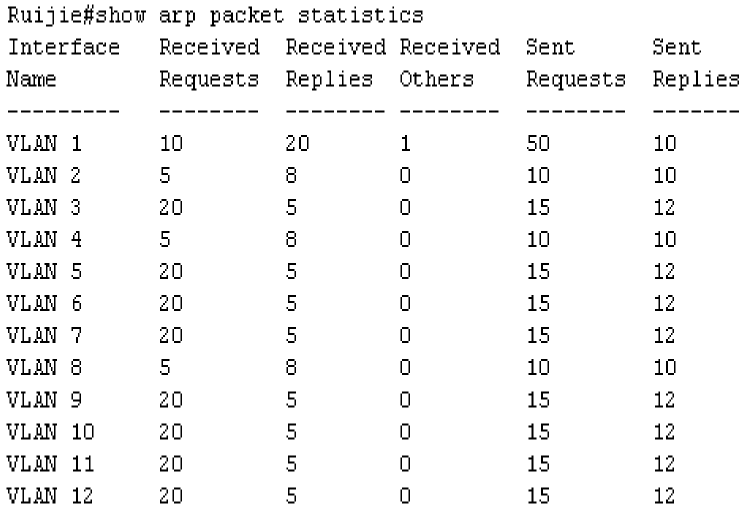
Parameter	**Description**
interface-name	Show the statistics of ARP packets on the specified interface.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples



```
Ruijie#show arp packet statistics
Interface   Received  Received Received  Sent      Sent
Name        Requests  Replies  Others    Requests  Replies
---------   --------  -------- --------  --------  -------
VLAN 1      10        20       1         50        10
VLAN 2      5         8        0         10        10
VLAN 3      20        5        0         15        12
VLAN 4      5         8        0         10        10
VLAN 5      20        5        0         15        12
VLAN 6      20        5        0         15        12
VLAN 7      20        5        0         15        12
VLAN 8      5         8        0         10        10
VLAN 9      20        5        0         15        12
VLAN 10     20        5        0         15        12
VLAN 11     20        5        0         15        12
VLAN 12     20        5        0         15        12
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

show arp timeout

Use this command to show the aging time of a dynamic ARP entry on the interface.

show arp timeout

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Any.

Usage Guide N/A.

Configuration Examples The following is the output of the **show arp timeout** command:

```
Ruijie# show arp timeout
Interface             arp timeout(sec)
----------------------  ----------------
```

```
VLAN 1               3600
```

The meaning of each field in the ARP cache table is described in Table 1.

Related Commands

Command	Description
N/A.	N/A.

Platform Description

show ip arp

Use this command to show the Address Resolution Protocol (ARP) cache table in the privileged user mode.

show ip arp

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following is the output of **show ip arp**:

```
Ruijie# show ip arp
Protocol Address      Age(min)Hardware      Type   Interface
Internet 192.168.7.233  23    0007.e9d9.0488  ARPA FastEthernet
0/0
Internet 192.168.7.112  10    0050.eb08.6617  ARPA FastEthernet
0/0
Internet 192.168.7.79   12    00d0.f808.3d5c  ARPA FastEthernet
0/0
Internet 192.168.7.1    50    00d0.f84e.1c7f  ARPA FastEthernet
0/0
Internet 192.168.7.215  36    00d0.f80d.1090  ARPA FastEthernet
0/0
Internet 192.168.7.127  0     0060.97bd.ebee  ARPA FastEthernet
0/0
Internet 192.168.7.195  57    0060.97bd.ef2d  ARPA FastEthernet
0/0
Internet 192.168.7.183  --    00d0.f8fb.108b  ARPA FastEthernet
```

```
0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

Related Commands

Command	Description
N/A.	N/A.

Platform Description

show ip interface

Use this command to show the IP status information of an interface. The command format is as follows:

show ip interface [*interface-type interface-number* | **brief**]

Parameter Description

Parameter	Description
interface-type	Specify interface type.
interface-number	Specify interface number.
brief	Show the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)

Defaults N/A.

Command Privileged EXEC mode.

Mode

Usage Guide

When an interface is available, RGOS will create a direct route in the routing table. The interface is available in that the RGOS software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the RGOS software removes the appropriate direct route from the routing table.

If the interface is unavailable, for example, two-way communication is allowed, the line protocol status will be shown as “UP”. If only the physical line is available, the interface status will be shown as “UP”.

The results shown may vary with the interface type, because some contents are the interface-specific options

Configuration Examples

Presented below is the output of the **show ip interface brirf** command:

```
Ruijie#show ip interface brief
Interface             IP-Address(Pri)   IP-Address(Sec)  Status
Protocol
GigabitEthernet 0/10  2.2.2.2/24     3.3.3.3/24    down    down
GigabitEthernet 0/11  no address     no address    down    down
VLAN 1                1.1.1.1/24     no address    down    down
```

Presented below is the output of the **show ip interface vlan** command.

```
SwitchA#show ip interface vlan 1
VLAN 1
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    1.1.1.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is:
  Proxy ARP is: OFF
ARP packet input number:         0
    Request packet:              0
    Reply packet:                0
    Unknown packet:            0
TTL invalid packet number:         0
ICMP packet input number:          0
    Echo request:                0
Echo reply:                   0
    Unreachable:                 0
    Source quench:                0
    Routing redirect:               0
```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface hardware status and line protocol status are “UP”.
IP interface type is:	Show the interface type, such as broadcast, point-to-point, etc.
IP interface MTU is:	Show the MTU value of the interface.
IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-broadcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachabled is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fast switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
ARP packet input number: 0 Request packet: 0	Show the total number of ARP packets received on the interface, including: ARP request packet

Reply packet: 0 Unknown packet: 0	ARP reply packet Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: 0 Echo request: 0 Echo reply: 0 Unreachable: 0 Source quench: 0 Routing redirect: 0	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet
Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A.

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
interface-name	Interface name
total	Show the total statistics of all interfaces.

Defaults N/A.

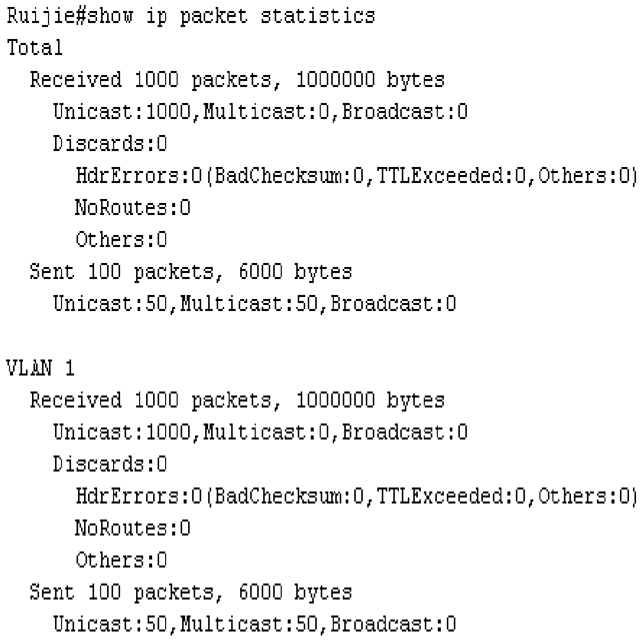
Command Mode

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	Configure the default gateway, which is only supported on the Layer 2 switch.

Platform Description

N/A.

IPv6 Configuration Commands

clear ipv6 neighbors

Use this command to clear the dynamically learned neighbors.

clrear ipv6 neighbors

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

This command can be used to clear all the neighbors dynamically learned by the neighbor discovering. Note that the static neighbors will not be cleared.

Configuration Examples

```
Ruijie# clear ipv6 neighbors
```

Related Commands

Command	Description
ipv6 neighbor	Configure the neighbor.
show ipv6 neighbors	Show the neighbor information.

Platform Description

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
iipv6-prefix	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
ipv6-address	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
prefix-length	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128.
prefix-name	The general prefix name. Use the specified general prefix to generate the interface address.
sub-bits	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
eui-64	The generated IPV6 address consists of the address prefix and the 64 bit interface ID

Defaults N/A

Command Mode Interface configuration mode

Usage Guide When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.

The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.

If no deleted address is specified when using **no ipv6 address**, all the manually configured addresses will be deleted.

no ipv6 address *ipv6-prefix*I*prefix-length* **eui-64** can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix*I*prefix-length* **eui-64**.

Configuration Examples

```
Ruijie(config-if)# ipv6 address 2001:1::1/64
Ruijie(config-if)# no ipv6 address 2001:1::1/64
Ruijie(config-if)# ipv6 address 2002:1::1/64 eui-64
Ruijie(config-if)# no ipv6 address 2002:1::1/64 eui-64
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

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 auto-configured address.

ipv6 address autoconfig[default]

no ipv6 address autoconfig

Parameter Description

Parameter	Description
default	(Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the **default** keyword

Defaults

N/A

Command Mode

Interface configuration mode

Usage Guide

The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address.

If the RA message contains the flag of the “other configurations”, the interface will obtain these “other configurations” through the DHCPv6. The “other configurations” usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc.

Use the **no ipv6 address autoconfig** command to delete the IPv6 address.

Configuration Examples

```
Ruijie(config-if)# ipv6 address autoconfig default
Ruijie(config-if)# no ipv6 address autoconfig
```

Related Commands

Command	Description
ipv6 address ipv6-*prefix/prefix-length* [**eui-64**]	Configure the IPv6 address for the interface manually .

Platform Description

N/A

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

Disabled.

Command Mode

Interface configuration mode.

Usage Guide

The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.

⚠ 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 Examples

```
Ruijie(config-if)#  ipv6 enable
```

Related Commands

Command	**Description**
show ipv6 interface	Show the related information of an interface.

Platform Description

N/A

ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

no ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

Parameter Description

Parameter	**Description**
prefix-name	The general prefix name.
pv6-prefix	The network prefix value of the general-prefix following the format defined in RFC4291.
prefix-length	The length of the general prefix.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.

A general prefix could contain multiple prefixes.

These longer specified prefixes is usually used for the Ipv6 address configuration on the interface.

Configuration Examples

The following example configures manually a general prefix as my-prefix.

```
Ruijie(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

Related Commands

Command	Description
ipv6 address *prefix-name sub-bits/prefix-length*	Configure the interface address using the general prefix.
show ipv6 general-prefix	Show the general prefix.

Platform Description

N/A

ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

ipv6 hop-limit *value*

no ipv6 hop-limit

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default is 64.

Command Mode

Global configuration mode.

Usage Guide

This command takes effect for the unicast messages only, not for multicast messages.

Configuration Examples

```
Ruijie(config)# ipv6 hop-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IPv6 packet in interface configuration mode. The **no** form of this command is used to restore it to the default configuration.

ipv6 mtu *bytes*

no ipv6 mtu

Parameter Description

Parameter	Description
bytes	Maximum transmission unit of IPv6 packet ranging 1280 to 1500 bytes

Defaults

It is the same as the value configured in the interface command **mtu** by default.

Command Mode

Interface configuration mode

Usage Guide

If an IPv6 packet is greater than the IPv6 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.

Configuration Examples

The following is an example of setting the IPy6 MTU value of the fastEthernet 0/1 interface to 1400 bytes.

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 mtu 1400
```

Related Commands

Command	Description
mtu	Set the MTU value of an interface.

Platform Description

N/A

ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.

ipv6

no

Parameter Description

Parameter	Description
value	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

Defaults 1.

Command Mode Interface configuration mode.

Usage Guide When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the ”tentative” status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

Configuration Examples

```
Ruijie(config-if)# ipv6 nd dad attempts 3
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.

Platform Description N/A

ipv6 nd dad retry

Use this command to set the address conflict detection interval for the conflict IPv6 address. Use the **no** form of this command to restore the default setting.

ipv6 nd dad retry *value*

no ipv6 nd dad retry

Parameter Description

Parameter	Description
value	Set the address conflict detection interval for the conflict IPv6

	address, 60s by default. The value 0 suggests that the address conflict detection is disabled. The value is within the range from 0 to 7200 in the unit of seconds.

Defaults 60s

Command Mode Global configuration mode.

Usage Guide Misoperations during configuration of IPv6 addresses may cause address conflicts. The conflict IPv6 address cannot be used immediately after the conflict is addressed. This command is used to trigger the address conflict detection to reuse the conflict IPv6 address once the conflict is addressed.

If there is no conflict found with the interface local address, the IPv6 protocol will be enabled on the interface and the address conflict detection will be performed for other IPv6 global addresses on the interface.

If the conflict is found again during detection, the log is printed like this: `%IPV6-3-DAD_FAILED: Duplicate 1000::1 was detected on interface Serial 3/0`.

Configuration Examples

```
Ruijie(config)# ipv6 nd dad retry 30
```

Related Commands

Command	Description
ipv6 nd dad attempts	Set the number of NSs sent during address conflict detection.

Platform Description 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 None.

Command Mode Interface configuration mode.

Usage Guide

This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.

Configuration Examples

```
Ruijie(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd other-config-flag	Set the flag for obtaining all information except IP address through stateful auto configuration.

Platform Description

N/A

ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore it to the default setting.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Parameter Description

Parameter	Description
milliseconds	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds

Defaults

The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000ms(1s).

Command mode

Interface configuration mode.

Usage Guide

The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

Configuration Examples

```
Ruijie(conifig-if)# ipv6 nd ns-interval 2000
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.

Platform Description N/A

ipv6 nd other-config-flag

Use this command to set “other stateful configuration” flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameter Description

Parameter	Description
N/A	N/A

Defaults The flag bit is not set by default.

Command mode Interface configuration mode.

Usage Guide With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

Configuration Examples

```
Ruijie(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.

Platform Description 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

Parameter	Description

Description

ipv6-prefix	IPv6 network ID following the format defined in RFC4291
prefix-length	Length of the IPv6 prefix. “/” shall be added in front of the prefix
valid-lifetime	Valid lifetime of the RA prefix received by the host
preferred-lifetime	Preferred lifetime of the RA prefix received by the host
at *valid-date preferred-date*	Set the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
infinite	Indicate that the prefix is always valid.
default	Set the default prefix.
no-advertise	The prefix will not be advertised by the device.
off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
no-autoconfig	Indicate that the RA prefix received by the host cannot be used for auto address configuration.

Defaults

By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:
valid-lifetime: 2592000s (30 days)
preferred-lifetime: 604800s (7 days),
The prefix is advertised and is used for on-link judgment and auto address configuration.

Command Mode

Interface configuration mode.

Usage Guide

This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

ipv6 nd prefix default

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

at *valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

Configuration Examples

The following example adds a prefix for SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(conifig-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 prefix default no-autoconfig
```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related Commands

Command	Description
show ipv6 interface	Show the RA information of an interface.

Platform Description N/A

ipv6 nd ra-hoplimit

Use this command to set the hopcount of the RA message. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-hoplimit *value*

no ipv6 nd ra-hoplimit

Parameter Description

Parameter	Description
value	Hopcount

Defaults The default value is 64.

Command Mode Interface configuration mode.

Usage Guide It is used to set the hopcount of the RA message.

Configuration Examples

```
Ruijie(config -if)# ipv6 nd ra-hoplimit 110
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd ra-lifetime	Set the lifetime of the device.
ipv6 nd ra-interval	Set the interval of sending the RA message.
ipv6 nd ra-mtu	Set the MTU of the RA message.

Platform Description N/A

ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore it to the default setting.

ipv6 nd ra-interval { *seconds* | **min-max** *min_value max_value* }

no ipv6 nd ra-interva l

Parameter Description

Parameter	Description
seconds	Interval of sending the RA message in seconds.
min-max	Maximum and minimum interval sending the RA message in seconds
min_value	Minimum interval sending the RA message in seconds
max_value	Maximum interval sending the RA message in seconds

Defaults

200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.

Command Mode

Interface configuration mode.

Usage Guide

If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

Configuration Examples

```
Ruijie(conifig-if)# ipv6 nd ra-interval 110
Ruijie(config-if)# ipv6 nd ra-interval min-max 110 120
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.
ipv6 nd ra-lifetime	Set the lifetime of the device.
ipv6 nd ra-hoplimit	Set the hopfcount of the RA message.
ipv6 nd ra-mtu	Set the MTU of the RA message.

Platform Description

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 it to the default setting.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameter Description

Parameter	**Description**
seconds	Default life time of the device on the interface

Defaults 1800s.

Command Mode Interface configuration mode.

Usage Guide The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

Configuration Examples

```
Ruijie(conifig-if)# ipv6 nd ra-lifetime 2000
```

Related Commands

Command	**Description**
show ipv6 interface	Show the interface information.
ipv6 nd ra-interval	Set the interval of sending the RA.
ipv6 nd ra-hoplimit	Set the hopcount of the RA.
ipv6 nd ra-mtu	Set the MTU of the RA.

Platform Description N/A

ipv6 nd ra-mtu

Use this command to set the MTU of the RA. Use the **no** form of this command to restore it to the default setting

ipv6 nd ra-mtu *value*

no ipv6 nd ra-mtu

Parameter Description

Parameter	**Description**
value	MTU value

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	Show the interface information.
ipv6 nd ra-lifetime	Set the lifetime of the device.
ipv6 nd ra-interval	Set the interval of sending the RA message.
ipv6 nd ra-hoplimit	Set the hopcount of the RA message.

Platform Description

N/A

ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore it to the default setting.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Parameter Description

Parameter	Description
milliseconds	Reachable time for the neighbor in the range 0 to 3,600,000 milliseconds.

Defaults

The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30,000ms(30s) when the device discovers the neighbor.

Command Mode

Interface configuration mode.

Usage Guide

The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time.

The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.

According to RFC4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5*configured value to 1.5*configured value.

Configuration

```
Ruijie(config-if)# ipv6 nd reachable-time 1000000
```

Examples

Related Commands

Command	Description
show ipv6 interface	Show the interface information.

Platform Description 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 function.

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 sending the RA message on an interface.

Configuration Examples

```
Ruijie(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.

Platform Description 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 RFC4291.
interface-id	Network interface of the neighbor (including routed Port, or SVI interface).
hardware-address	Hardware address of the neighbor. It shall 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, the static neighbor can only be configured on an IPv6 protocol enabled interface.

If the neighbor to be configured has been learned through NDP and has been stored in the neighbor list, the dynamically generated neighbor will be automatically switched to a static one. The configured static neighbor is always in the **Reachable** status.

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	Show the neighbor information.
clear ipv6 neighbors	Clear the neighbors learned dynamically.

Platform Description

N/A

ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. When **no ipv6 ns-linklocal-src** is executed, the global IP address will be taken as the source address to send neighbor requests.

ipv6 ns-linklocal-src

no ipv6 ns-linklocal-src

Parameter Description

Parameter	Description

N/A	N/A

Defaults

The local address of the link is always used as the source address to send neighbor requests.

Command Mode

Global configuration mode.

Usage Guide

None.

Configuration Examples

```
Ruijie(config)# no ipv6 ns-linklocal-src
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to 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 any ICMPv6 error message is limited. By default, it is 10pps.

Configuration Examples

```
Ruijie(config-if)# ipv6 redirects
```

Related Commands

Command	Description
show ipv6 interface	Show the interface information.

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 setting.

ipv6 route *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-id* [*ipv6-address* } [*distance*]

Parameter Description

Parameter	Description
ipv6-prefix	IPV6 network number following the format specified in RFC4291. prefix-length: Length of the IPv6 prefix. "/" must be added in front of the prefix.
ipv6-address	Next-hop IP address to the destination address. It shall be in the format defined in RFC4291. 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 toward 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 on the link connected with the outgoing interface; that is to say, the static route will be treated as a directly-connected route. Note that if the destination network or next-hop address is a link-local address, the outgoing interface must be specified.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

Note

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 be also a link-local IP address. When configuring a route, the destination IP address and the next-hop IP address shall not 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 shall be the same as the configured outgoing interface.

Configuration

```
Ruijie(config)# ipv6 route 2001::/64 vlan 1 2005::1
```

Examples

Related Commands

Command	Description
show ipv6 route	Show the IPv6 route information.

Platform Description

N/A

ipv6 source-route

Use this command to forward the IPv6 packet with route header. The **no** form of this command disables the forwarding.

ipv6 source-route

no ipv6 source-route

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled.

Command Mode

Global configuration mode.

Usage Guide

Because of the potential security of the header of type 0 route, it’s easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.

Configuration Examples

```
Ruijie(config)# no ipv6 source-route
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ping ipv6

Use this command to diagnose the connectivity of the 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, the 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 regulated 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 status, or the IPv6 function is disabled on the interface (for example, IP address collision is detected).
?	Unknown error

Configuration Examples

```
Ruijie# ping ipv6 fec0::1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show ipv6 address

Use this command to show the IPv6 addresses.

show ipv6 address [*interface-name*]

Parameter Description

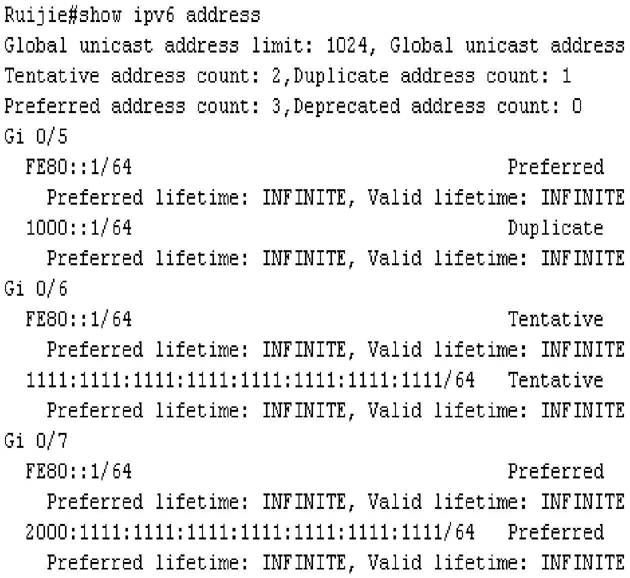
Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

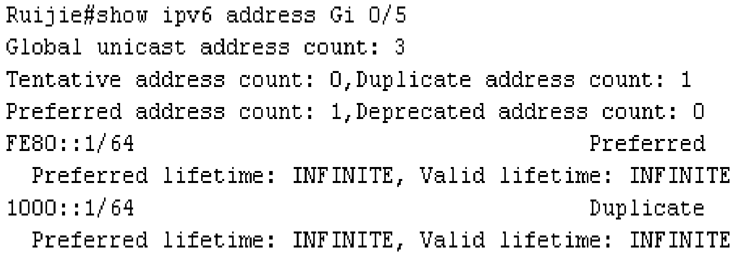
Usage Guide N/A

Configuration Examples The following example shows all IPv6 address configured on the device.



```
Ruijie#show ipv6 address
Global unicast address limit: 1024, Global unicast address count: 3
Tentative address count: 2,Duplicate address count: 1
Preferred address count: 3,Deprecated address count: 0
Gi 0/5
  FE80::1/64                                   Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  1000::1/64                                   Duplicate
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Gi 0/6
  FE80::1/64                                   Tentative
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  1111:1111:1111:1111:1111:1111:1111:1111/64   Tentative
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Gi 0/7
  FE80::1/64                                   Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  2000:1111:1111:1111:1111:1111:1111:1111/64   Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

The following example shows the IPv6 address configured on the GigabitEthernet 0/1.



```
Ruijie#show ipv6 address Gi 0/5
Global unicast address count: 3
Tentative address count: 0,Duplicate address count: 1
Preferred address count: 1,Deprecated address count: 0
FE80::1/64                                    Preferred
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
1000::1/64                                    Duplicate
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 general-prefix

Use this command to show 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 show the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

Configuration Examples The following example shows 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	Configure the general prefix.

Platform Description N/A

show ipv6 interface

Use this command to show the IPv6 interface information.

show ipv6 interface [*interface-id*] [**ra-info**]

Parameter Description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregateport, or SVI)
ra-info	Show the RA information of the interface.

Defaults N/A v

Command Mode Privileged EXEC mode.

Usage Guide Use this command to show the address configuration, ND configuration and other 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: 2001::1, subnet is 2001::/64 [**TENTATIVE**]. The flag bit in the [ ] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.

```
Ruijie# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags: LA)
```

Description of the fields in **ra-info**:

Field	Meaning
RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.
initcount	Indicate the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M | M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O | O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	Meaning
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicate that the interfaces use the default prefix.
Auto | CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.
vltime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.
L | !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A | !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

show ipv6 neighbors

Use this command to show the IPv6 neighbors.

show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]

show ipv6 neighbors static

Parameter Description

Parameter	**Description**
verbose	Show the neighbor details.
static	Show the validity status of static neighbors.
interface-id	Show the neighbors of the specified interface.
ipv6-addres	Show the neighbors of the specified IPv6 address.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Show the neighbors on the SVI 1 interface:

```
Ruijie# show ipv6 neighbors vlan 1
IPv6 Address Linklayer Addr   Interface
fa::1        00d0.0000.0002   vlan 1
fe80::200:ff:fe00:2  00d0.0000.0002  vlan 1
Show the neighbor details:
Ruijie# show ipv6 neighbors verbose
IPv6 Address  Linklayer Addr Interface
2001::1      00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1    00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
```

Field	Meaning
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.
Interface	Interface the neighbor locates.
State	State of the neighbor: state/H(R) The values of STATE are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start

	NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3). ?: Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.
Age	The reachable time of the neighbor. ’-‘ indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. ’expired’ indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

Configuration Examples

```
Ruijie# show ipv6 neighbors
```

Related Commands

Command	Description
ipv6 neighbor	Configure a neighbor.

Platform Description

N/A

show ipv6 neighbors statistics

Use the following command to show the statistics of one IPv6 neighbors.

show ipv6 neighbors statistics

Use the following command to show the statistics of all IPv6 neighbors.

show ipv6 neighbors statistics all

Parameter Description

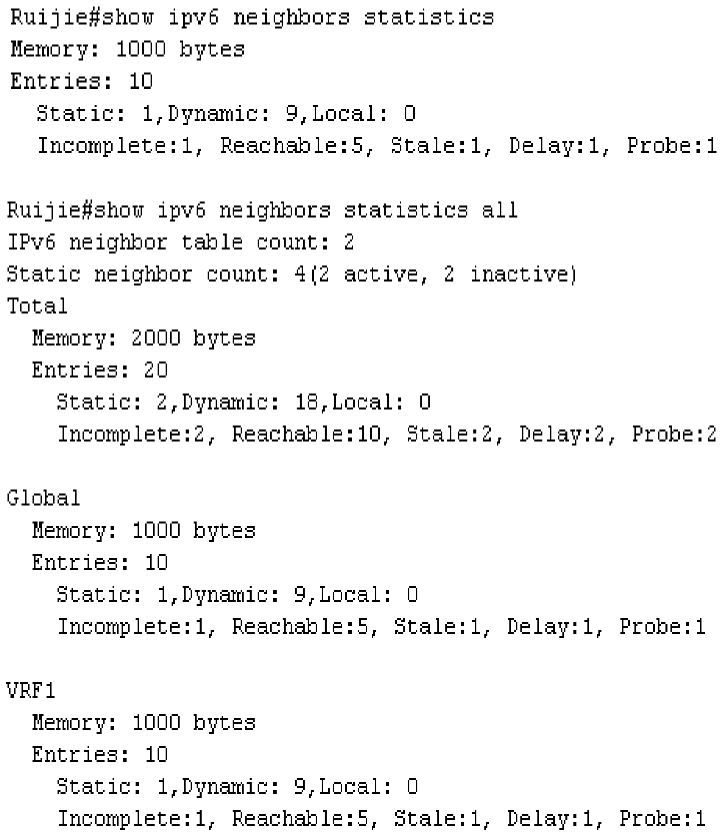
Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example shows the statistics of the global neighbors.



```
Ruijie#show ipv6 neighbors statistics
Memory: 1000 bytes
Entries: 10
  Static: 1,Dynamic: 9,Local: 0
  Incomplete:1, Reachable:5, Stale:1, Delay:1, Probe:1

Ruijie#show ipv6 neighbors statistics all
IPv6 neighbor table count: 2
Static neighbor count: 4(2 active, 2 inactive)
Total
  Memory: 2000 bytes
  Entries: 20
    Static: 2,Dynamic: 18,Local: 0
    Incomplete:2, Reachable:10, Stale:2, Delay:2, Probe:2

Global
  Memory: 1000 bytes
  Entries: 10
    Static: 1,Dynamic: 9,Local: 0
    Incomplete:1, Reachable:5, Stale:1, Delay:1, Probe:1

VRF1
  Memory: 1000 bytes
  Entries: 10
    Static: 1,Dynamic: 9,Local: 0
    Incomplete:1, Reachable:5, Stale:1, Delay:1, Probe:1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

show ipv6 packet statistics

Use this command to show the statistics of IPv6 packets.

show ipv6 packet statistics [**total** | *interface-name*]

Parameter

Parameter	Description

Description

total	Show total statistics of all interfaces.
interface-name	Interface name

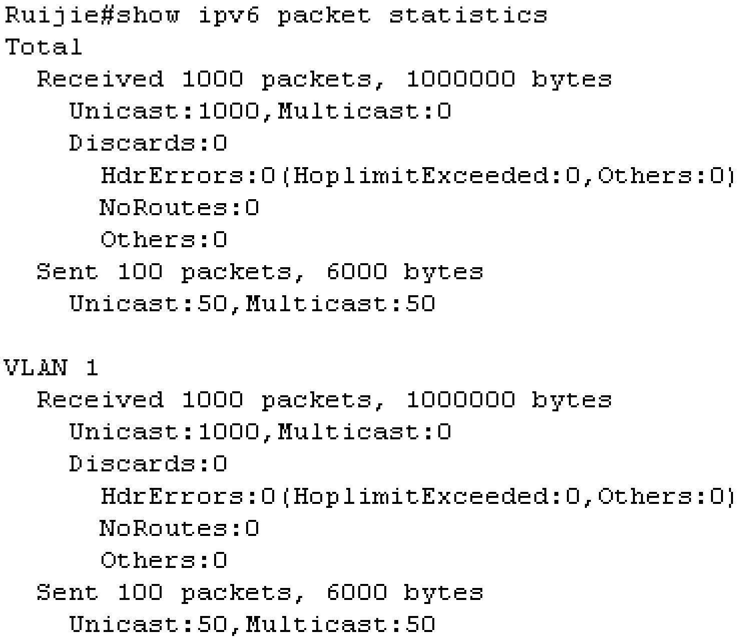
Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

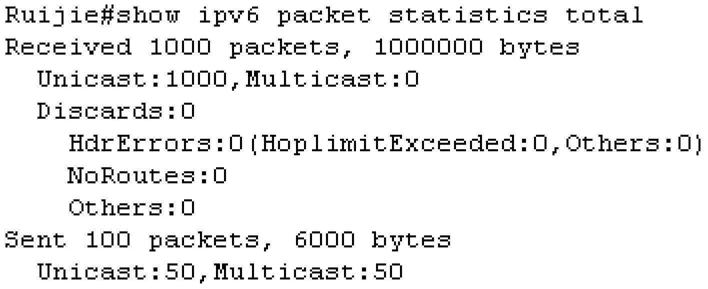
The following example shows the total statistics of the Ipv6 packets and the statistics of each inerface.



```
Ruijie#show ipv6 packet statistics
Total
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50

VLAN 1
  Received 1000 packets, 1000000 bytes
    Unicast:1000,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 100 packets, 6000 bytes
    Unicast:50,Multicast:50
```

The following example shows the total statistics of the Ipv6 packets.



```
Ruijie#show ipv6 packet statistics total
Received 1000 packets, 1000000 bytes
  Unicast:1000,Multicast:0
  Discards:0
    HdrErrors:0(HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:0
Sent 100 packets, 6000 bytes
  Unicast:50,Multicast:50
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

show ipv6 route

Use this command to show the IPv6 route information.

show ipv6 route [**static** | **local** | **connected**]

Parameter Description

Parameter	Description
static	Show the static routes.
local	Show the local routes.
connected	Show the directly-connected routes.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to view 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	Configure a static route.

Platform Description N/A

show ipv6 route summary

Use the following command to show the statistics of one IPv6 route table.

show ipv6 route summary

Use the following command to show the statistics of all IPv6 route tables.

show ipv6 route summary all

Parameter Description

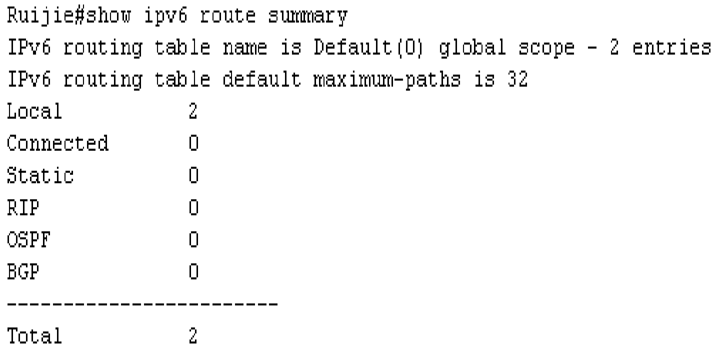
Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

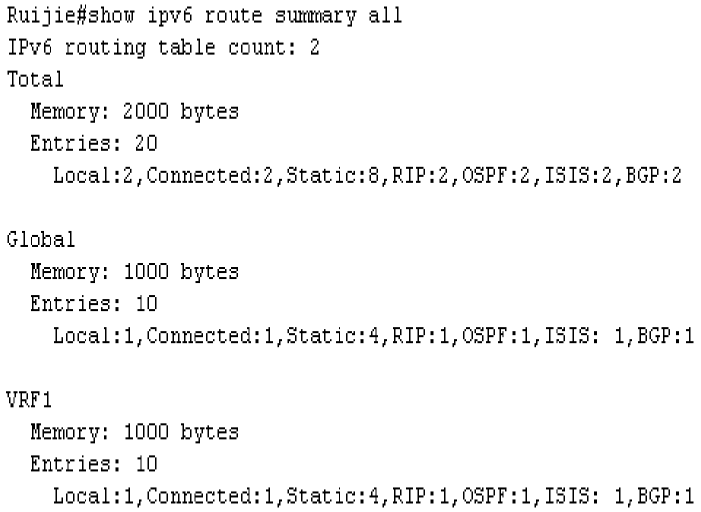
Usage Guide N/A

Configuration Examples The following example shows the statistics of the global route 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 shows the statistics of all route 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	Configure a static route.

Platform Description

N/A

show ipv6 routers

In the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to show the neighbor routers and the advertisement.

show ipv6 routers [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type *interface-number*	(Optional) Show the routing advertisement of the specified interface.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to show the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.

Configuration Examples

The following example shows the IPv6 router

```
Ruijie# show ipv6 routers
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
```

```
Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
Preference=MEDIUM
Reachable time 0 msec, Retransmit time 0 msec
Prefix 6001:3::/64 onlink autoconfig
  Valid lifetime 2592000 sec, preferred lifetime 604800 sec
Prefix 6001:2::/64 onlink autoconfig
  Valid lifetime 2592000 sec, preferred lifetime 604800 sec
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

DHCP Configuration Commands

clear ip dhcp relay statistics

Use this command to reset the DHCP relay counters.

clear ip dhcp relay statistics

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie# clear ip dhcp relay statistics
```

Related Commands

Command	Description
show ip dhcp relay statistics	Show the DHCP relay counters.

Platform Description N/A

debug ip dhcp client

Use this command to carry out the DHCP client debugging in the privileged user mode. Use the **no** form of this command to disable the DHCP client debugging function.

debug ip dhcp client

no debug ip dhcp client

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command Mode Privileged EXEC mode.

Usage Guide

This command is used to show the main message content of the DHCP client during the interaction of the servers and the processing status.

Configuration Examples

The example below turns on the debugging switch of the DHCP client in the equipment.

```
debug ip dhcp client
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ip address dhcp

Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. The **no** form of this command can be used to cancel this configuration.

ip address dhcp

no ip address dhcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The interface cannot obtain the ID address by the DHCP by default.

Command Mode

Interface configuration mode.

Usage Guide

When requesting the IP address, the DHCP client of the RGOS software also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information (optional).

The client of the RGOS software is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server. At present, our server can support this function.

Configuration Examples

The configuration example below makes the FastEthernet 0 port obtain the IP address automatically.

interface fastEthernet 0

```
ip address dhcp
```

Related Commands

Command	Description
dns-server	Define the DNS server of DHCP client.
ip dhcp pool	Define the name of the DHCP address pool and enter the DHCP address pool configuration mode.

Platform Description

N/A

ip dhcp relay check server-id

Use this command to enable the **ip dhcp relay check** *server-id* function. The **no** form of this command is used 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

Disabled.

Command Mode

Global configuration mode.

Usage Guide

Switch will select the server to be sent according to server-id option when forwarding DHCP REQUEST via this command. Without this command configured, the switch forwards the DHCP REQUEST to all configured DHCP servers.

Configuration Examples

The following example enables the ip dhcp relay check server-id function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay check server-id
```

Related Commands

Command	Description
service dhcp	Enable the DHCP Relay.

Platform Description

N/A

ip dhcp relay information option dot1x

Use this command to enable the **dhcp option dot1x** function. The **no** form of the command is used to disable the **dhcp option dot1x** function.

ip dhcp relay information option dot1x

no ip dhcp relay information option dot1x

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled.

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	Enable the DHCP Relay.
ip dhcp relay information option dot1x access-group	Configure the option dot1x acl.

Platform Description

N/A

ip dhcp relay information option dot1x access-group

Use this command to configure the **dhcp option dot1x acl**. The **no** form of this command is used to disable the **dhcp option dot1x acl**.

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 with.

Command Mode

Global configuration mode.

Usage Guide

Be sure 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	Enable the 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 **ip dhcp relay information option82** function. The **no** form of this command is used to disable the **ip dhcp relay information option82** function.

ip dhcp relay information option82

no ip dhcp relay information option82

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled.

Command Mode

Global configuration mode.

Usage Guide

This command is exclusive with the **option dot1x** command.

Configuration Examples

The following example enables the option82 function on the DHCP relay.

```
Ruijie# configure terminal
```

```
Ruijie(config)# Ip dhcp relay information option82
```

Related Commands

Command	Description
service dhcp	Enable the DHCP Relay.

Platform Description N/A

ip dhcp relay suppression

Use this command to enable the DHCP binding globally. The **no** form of this command disables the DHCP binding globally and enables the **DHCP relay** suppression on the port.

ip dhcp relay suppression

no ip dhcp relay suppression

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command Mode Interface configuration mode.

Usage Guide After executing this command, the system will not relay the DHCP request message on the interface.

Configuration Examples The following example enables the relay suppression function on the interface 1.

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp relay suppression
Ruijie(config-if)# exit
Ruijie(config)#
```

Related Commands

Command	Description
service dhcp	Enable the DHCP Relay.

Platform Description N/A

ip helper-address

Use this command to add an IP address of the DHCP server. The **no** form of this command deletes an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

ip helper-address {cycle-mode |A.B.C.D}

no ip helper-address {cycle-mode |A.B.C.D}

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode, interface configuration mode.

Usage Guide Up to 20 DHCP server IP addresses can be configured globally or on a layer-3 interface.

One DHCP request of this interface will be sent to these servers. You can select one for confirmation.

Configuration Examples N/A

Related Commands

Command	Description
service dhcp	Enable the DHCP relay.

Platform Description N/A

Platform Description N/A

service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in global configuration mode. The **no** form of this command can be used to disable the DHCP server and the DHCP relay.

service dhcp

no service dhcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Global configuration mode.

Usage Guide The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.

Configuration Examples

In the following configuration example, the device has enabled the DHCP server and the DHCP relay feature.

```
service dhcp
```

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.

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, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address.

Configuration Examples

The following is the result of the show dhcp lease.

```
Ruijie# show dhcp lease
Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0
Temp sub net mask: 255.255.255.0
 DHCP Lease server: 192.168.5.70, state: 3 Bound
 DHCP transaction id: 168F
 Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
 Next timer fires after: 00:04:29
 Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Fa0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ip dhcp relay statistics

Use this command to show the DHCP relay counters.

show ip dhcp relay statistics

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie#sh ip dhcp relay-s
Cycle mode              0

Message                Count
Discover               0
Offer                 0
Request                0
Ack                   0
Nak                   0
Decline                0
Release                0
Info                  0
Bad                   0

Direction              Count
Rx client              0
Rx client uni           0
Rx client bro           0
Tx client              0
Tx client uni           0
Tx client bro           0
Rx server              0
Tx server              0
```

Related

Command	Description

Commands

clear ip dhcp relay statistics	Reset the DHCP relay counters.

Platform Description N/A

DHCPv6 Configuration Commands

clear ipv6 dhcp client

Use this command to reset the DHCPv6 client.

clear ipv6 dhcp client *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type *interface-number*	Set the interface type and the interface number.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

This command is used to restart the DHCPv6 client, which may lead the client to request for the configurations from the server again.

Configuration Examples

```
Ruijie# clear ipv6 dhcp client vlan 1
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

ipv6 dhcp client pd

Use this command to enable the DHCPv6 client and request for the prefix address information. Use the **no** form of this command to disable the prefix address request

ipv6 dhcp client pd *prefix-name* [**rapid-commit**]

no ipv6 dhcp client pd

Parameter Description

Parameter	Description
prefix-name	Define the IPv6 prefix name.

rapid-commit	Allow the simplified interaction process.

Defaults Disabled

Command Mode Interface configuration mode.

Usage Guide With the DHCPv6 client mode disabled, use this command to enable the DHCPv6 client mode on the interface.

With the **ipv6 dhcp client pd** command enabled, the DHCPv6 client sends the prefix request to the DHCPv6 server

The keyword **rapid-commit** allows the client and the server two-message interaction process. With this keyword configured, the solicit message sent by the client includes the **rapid-commit** item.

Configuration Examples The following example shows how to enable the prefix information request on the interface:

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 dhcp client pd pd_name
```

Related Commands

Command	Description
clear ipv6 dhcp client	Reset the DHCPv6 client function on the interface.
show ipv6 dhcp interface	Show the DHCPv6 interface configuration.

Platform Description N/A

show ipv6 dhcp

Use this command to show the device DUID.

show ipv6 dhcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide The server, client and relay on the same device share a DUID.

Configuration

```
Ruijie# show ipv6 dhcp
```

Examples

```
This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show ipv6 dhcp interface

Use this command to show the DHCPv6 interface information.

show ipv6 dhcp interface [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Set the interface name.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

If the *interface-name* is not specified, all DHCPv6 interface information is shown. If the *interface-name* is specified, the specified interface information is shown.

Configuration Examples

```
Ruijie# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool dhcp-pool
  Rapid-Commit: disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

DNS Configuration Commands

clear host

Use this command to clear the dynamically learned host name in the privileged user mode.

clear host [*host-name*]

Parameter Description

Parameter	Description
host-name	Delete the dynamically learned host. “*” denotes to clear all the dynamically learned host names.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** 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 configuration will delete the dynamically learned mapping records from the host name-IP address buffer table.

```
clear host *
```

Related Commands

Command	Description
show hosts	Show the host name buffer table.

Platform Description N/A

ip domain-lookup

Use this command to enable the DNS to carry out the domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

ip domain-lookup

no ip domain-lookup

Parameter Description

Parameter	Description

N/A	N/A

Defaults Enabled.

Command Mode Global configuration mode.

Usage Guide This command enables the domain name resolution function.

Configuration Examples The following example enables the DNS domain name resolution function.

```
Ruijie(config)# ip domain-lookup
```

Related Commands

Command	Description
show hosts	Show 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	The host name of the equipment
ip-address	The IP address of the equipment

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	Show the DNS related configuration information.

Platform Description N/A

ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server { *ip-address* | *ipv6-address }*

no ip name-server [*ip-address* | *ipv6-address*]

Parameter Description

Parameter	Description
ip-address	The IP address of the domain name server.
ipv6-address	The IPv6 address of the domain name server.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response.

Up to 6 DNS servers are supported. You can delete a DNS server with the *ip-address* option or all the DNS servers.

Configuration Examples

```
Ruijie(config)# ip name-server 192.168.5.134
Ruijie(config)# ip name-server
2001:0DB8::250:8bff:fee8:f800 2001:0DB8:0:f004::1
```

Related Commands

Command	Description
show hosts	Show 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	The host name of the equipment
ipv6-address	The IPv6 address of the equipment

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

To delete the host list, use the **no ipv6 host** *host-name ipv6-address* command.

Configuration Examples

```
Ruijie(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

Related Commands

Command	Description
show hosts	Show the DNS related configuration information.

Platform Description

N/A

show hosts

Use this command to display DNS configuration.

show hosts [*hostname*]

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Show the DNS related configuration information.

Configuration

```
Ruijie# show hosts
```

Examples

```
Name servers are:
192.168.5.134 static

Host             type        Address            TTL(sec)
switch            static      192.168.5.243         ---
www.ruijie.com   dynamic     192.168.5.123         126
```

Related Commands

Command	Description
ip host	Configure the host name and IP address mapping by manual.
ipv6 host	Configure the host name and IPv6 address mapping by manual.
ip name-server	Configure the DNS server.

Platform Description

N/A

FTP Server Configuration Commands

debug ftp server

Use this command to enable outputting the debugging messages in the FTP server. Use the **no** form of this command to disable this function.

debug ftpserve

no debug ftpserver

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Privileged user mode.

Usage Guide Use this command to display the detailed debugging information during FTP server operation.

Configuration Examples The following example shows how to enable outputting the debugging messages in the FTP Server:

```
Ruijie# debug ftpserver
FTPSRV_DEBUG:(RECV)   SYST
FTPSRV_DEBUG:(REPLY)  215 RGOS Type: L8
FTPSRV_DEBUG:(RECV)   PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY)  200 PORT Command okay.
```

The following example shows how to disable outputting the debugging messages in the FTP Server:

```
Ruijie# no debug ftpserver
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ftp-server enable

Use this command to enable the FTP server. Use the **no** form of this command to disable the FTP server.

ftp-server enable

no ftp-server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Global configuration mode.

Usage Guide This command is used to enable the FTP server to connect the FTP client to upload/download the files.

Caution

To enable the FTP client to access to the FTP server files, this command shall be co-used with the **ftp-server topdir** command.

Configuration Examples The following example shows how to enable the FTP Server and make the FTP client access to the syslog content only:

```
Ruijie(config)# ftp-server topdir /syslog
Ruijie(config)# ftp-server enable
```

The following example shows how to disable the FTP Server:

```
Ruijie(config)# no ftp-server enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ftp-server password

Use this command to set the login password for the FTP server. Use the **no** form of this command to cancel the password configuration.

ftp-server password [*type*] *password*

no ftp-server password

Parameter Description

Parameter	Description
type	Define the encryption type of the password: 0 or 7. The default type is

	0. 0 indicates the password is not encrypted. 7 indicates the password is encrypted.
password	The login password for the FTP server.

Defaults By default, there is no password.

Command Mode Global configuration mode.

Usage Guide For the FTP server, the login username and the login password must be configured to verify the client connection. One password can be set at most.

The password must include the letter or number. The space in front of / behind the password is allowed, but it is ignored. While the space in the middle of the password is a part of password.

The minimum and maximum lengths of the plain-text password are 1 character and 25 characters.

The minimum and maximum lengths of the encrypted password are 4 characters and 52 characters respectively.

The encrypted password is generated by plain-text password encryption and its format must comply with the encryption specification. If the encrypted password is used for the setting, the client must use the corresponding plain-text password for the purpose of successful login.

Caution

Null password is not supported by the FTP server. Without the password configuration, the client fails to pass the identity verification of the server.

Configuration Examples The following example shows how to set the plain-text password as pass:

```
Ruijie(config)# ftp-server password pass
```

OR:

```
Ruijie(config)# ftp-server password 0 pass
```

The following example shows how to set the cipher-text password as 8001:

```
Ruijie(config)# ftp-server password 7 8001
```

The following example shows how to delete the password configuration:

```
Ruijie(config)# no ftp-server password
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ftp-server timeout

Use this command to set the FTP session idle timeout. Use the **no** form of this command to restore the idle timeout to the default value 30 minutes

ftp-server timeout *time*

no ftp-server timeout

Parameter Description

Parameter	Description
time	Set the session idle timeout, in minutes. The valid range is 1-3600.

Defaults Default time is 30 minutes.

Command Mode Global configuration mode.

Usage Guide Use this command to set the FTP session idle timeout. If the session is idle, the FTP server deems the session connection is invalid and disconnects with the user.

Caution The session idle time refers to the time for the FTP session between two FTP operations

Configuration Examples The following example shows how to set the session idle timeout as 5 minutes:

```
Ruijie(config)# ftp-server timeout 5
```

The following example shows how to restore the session idle timeout to the default value (30 minutes):

```
Ruijie(config)# no ftp-server timeout
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ftp-server topdir

Use this command to set the directory range for the FTP client to access to the FTP server files. Use the **no** form of this command to prevent the FTP client from accessing to the FTP server files.

ftp-server topdir *directory*

no ftp-server topdir

Parameter Description

Parameter	Description
directory	Set the top-directory.

Defaults By default, no top-directory is configured.

Command Mode Global configuration mode.

Usage Guide The FTP server top directory specifies the directory range of the files accessed by the client. Can the FTP client accesses to the files on the FTP server with the top directory correctly specified.

Without this command configured, FTP client fails to access to any file or directory on the FTP server.

Configuration Examples The following example shows how to enable the FTP Server and make the FTP client access to the syslog content only:

```
Ruijie(config)# ftp-server topdir /syslog
Ruijie(config)# ftp-server enable
```

The following example shows how to remove the top-directory configuration:

```
Ruijie(config)# no ftp-server topdir
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ftp-server username

Use this command to set the login username for the FTP server. Use the **no** form of this command to cancel the username configuration.

ftp-server username *username*

no ftp-server username

Parameter Description

Parameter	Description
username	Set the login username.

Defaults By default, no username is set.

Command Mode Global configuration mode

Usage Guide

Use this command to set the login username for the FTP server. To log in to the FTP server, the correct username and password shall be provided.

The maximum length of the username is 64 characters and the spaces are not allowed in the middle of the username. The username consists of letters, semiangle number and semiangle mark. One username can be configured for the FTP server at most.

Caution

The anonymous user login is not supported on the FTP server. The client fails to pass the identity verification if the username is removed.

Configuration Examples

The following example shows how to set the username as user:

```
Ruijie(config)# ftp-server username user
```

The following example shows how to remove the username configuration:

```
Ruijie(config)# no ftp-server username
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show ftp-server

Use this command to show the status information of the FTP server.

show ftp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

The FTP server status information includes:

- Enabled/Disabled server
- The control connection is set up or not (the related IP, Port are shown)
- The data connection is set up or not (the related IP, Port and the working mode are shown)

- The current file transmission type
- The login username and password
- The FTP server top directory
- The session idle timeout setting

Configuration Examples

The following example shows the related status information of the FTP server:

```
Ruijie# show ftp-server
ftp-server information
=======================================
enable : Y
topdir : /
timeout: 20min
username config : Y
password config : Y
type: BINARY
control connect : Y
ftp-server: ip=192.167.201.245  port=21
ftp-client: ip=192.167.201.82  port=4978
port data connect : Y
ftp-server: ip=192.167.201.245  port=22
ftp-client: ip=192.167.201.82  port=4982
passive data connect : N
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

FTP Client Configuration Commands

copy ftp

This section introduces how to use the **copy ftp** command to transfer files at the CLI in the main program. To use the FTP client to download files to the device, execute the **copy ftp:url flash:url** command in the privileged mode. Use the **copy flash:url ftp:url** command to upload files of the local client to the server.

copy ftp://*username*:*password*@*dest-address* [/*remote-directory*]/*remote-file*
flash:[*local-directory/*]*local-file*
copy flash:[*local-directory/*]*local-file* **ftp:**//*username*:*password*@*dest-address* [/*remote-directory*]/ *remote-file*

Parameter Description

Parameter	Description
username	Username for logging in to the FTP server, with a length no more than 40 bytes. The username does not contain dot (.), at sign (@), slash (/), and space. This parameter is mandatory.
password	Password for logging in to the FTP server, with a length no more than 32 bytes. The password does not contain dot (.), at sign (@), slash (/), and space. This parameter is mandatory.
dest-address	IP address of the FTP server
remote-directory	Name of the optional directory on the FTP server for uploading files, with a length no more than 255 bytes. The directory name does not contain space and Chinese characters. If this parameter is empty, the current directory of the FTP server is used.
remote-file	Name of the file on the remote server, with a length no more than 255 bytes. The name does not contain space and Chinese characters.
local-directory	Optional directory of the folder on the local device. Create the folder on the local device before specifying the directory of the folder because this command cannot automatically create a folder. If this parameter is empty, the current directory is used, with a length no more than 255 bytes, and does not contain space and Chinese characters.
local-file	Name of the file on the local server, with a length no more than 255 bytes. The name does not contain space and Chinese characters.

Defaults -

Command Modes Privileged user mode

Usage Use the **copy ftp**:*url* **flash**:*url* command to download files.

Guidelines

Use the **copy flash**:*url* **ftp**: *url* command to upload files.

Examples

The username is **user**; password is **pass**, IP address is **192.168.23.69**. Download the file named **remote-file** under the root directory of the FTP server to the home directory of the device, and save it as **local-file**.

```
Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file
flash:home/local-file
```

Upload the file **local-file** under the home directory of the device to the root directory of the FTP server, and save it as **remote-file**.

```
Ruijie# copy flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

Related Commands

Command	Description
copy tftp	Uses TFTP to transfer files.

Platform Description

-

default ftp-client

Use the **default ftp-client** command to restore the default setting of the FTP client in the global configuration mode, namely, passive (PASV) mode for data connection, binary mode for file transfer, and client source IP address not bound.

default ftp-client

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The data connection mode is passive (PASV), file transfer mode is binary, and no local source IP address is specified.

Command Modes

Global configuration mode

Usage Guidelines

Use this command to restore the default setting of the FTP client.

Examples

Restore the default setting of the FTP client.

```
Ruijie (config)# default ftp-client
```

Related

Command	Description

Commands

-	-

Platform Description

-

ftp-client ascii

Use the **ftp-client ascii** command to set the FTP transfer mode to text (ASCII). Use the **no** form of this command to restore the default setting.

ftp-client ascii

no ftp-client ascii

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default FTP transfer mode is binary.

Command Modes

Global configuration mode

Usage Guidelines

This command sets the file transfer mode to the text (ASCII) mode.

Examples

Set the file transfer mode to ASCII.

```
Ruijie (config)# ftp-client ascii
```

Related Commands

Command	Description
-	-

Platform Description

-

ftp-client port

Use the **ftp-client port** command to set the FTP data connection mode to active (PORT). Use the **no** form of this command to restore the passive mode, in which the client initiates a connection to the server for data transmission.

ftp-client port

no ftp-client port

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default FTP connection mode is passive (PASV).

Command Modes Global configuration mode

Usage Guidelines You can use this command to set the active mode for data connection, in which the server initiates a connection to the client.

Examples Set the active mode for FTP connection.

```
Ruijie (config)# ftp-client port
```

Related Commands

Command	Description
-	-

Platform Description -

ftp-client source-address

Use the **ftp-client source-address** command to configure the source address of the FTP client for transmitted FTP packets.

Use the **no** form of this command to remove the binding.

ftp-client source-address {*ip-address* | *ipv6-address*}

no ftp-client source-address

Parameter Description

Parameter	Description
ip-address	IP address of the FTP client
ipv6-address	IPv6 address of the FTP client

Defaults By default, no source IP address is specified for the client. The device uses the IP address of the interface determined by the matched route as the source IP address to communicate with an FTP server.

Command Modes Global configuration mode

Usage Guidelines

This command configures a source IP address for a client to connect to the server.

Examples

Set the active mode for FTP connection.

```
Ruijie (config)# ftp-client source-address 192.168.23.236
```

Related Commands

Command	Description
-	-

Platform Description

-

Network Connectivity Test Tool Configuration 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 [**ip**] [*ip-address* [**length** *length*] [**ntimes** *times*] [t**imeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**]]

Parameter Description

Parameter	Description
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.
seconds	Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address.
df-bit	Sets the DF bit for the IP address. DF bit=1 indicates not to segmentate the datagrams. By default, the DF bit is 0.
validate	Sets whether to validate the reply packets or not.

Defaults

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

Command Mode

Privileged EXEC mode.

Usage Guide

The ping command can be used in the ordinary user mode and the privileged EXEC mode. In the ordinary mode, only the basic functions of ping are available. In the privileged EXEC mode, in addition to the basic functions, the extension functions of the ping are also available. For the ordinary functions of ping, five packets of 100Byte in length are sent to the specified IP address within the specified period (2s by default). If response is received, '!' is displayed. If no response is received, '.' displayed, and the statistics is displayed at the end. For the extension functions of ping, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Configuration Examples

The example below 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 example below shows the extension ping.
Ruijie# ping 192.168.5.197 length 1500 ntimes 100 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds, data
ffff source 192.168.4.10:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ping ipv6

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format as follows:

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

Parameter Description

Parameter	Description
ipv6-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: 127.0.0.1) is not allowed to be the source address.

Defaults

Five packets with 100 Bytes in length are sent to the specified IP address within specified time 2 seconds by default

Command Mode

Privileged EXEC mode.

Usage Guide

The **ping ipv6** command can be used in the ordinary user mode and the privileged EXEC mode. In the ordinary mode, only the basic functions of ping ipv6 are available. In the privileged EXEC mode, in addition to the basic functions, the extension functions of the ping ipv6 are also available. For the ordinary functions of ping ipv6, five packets of 100Byte in length are sent to the specified IP address within the specified period (2 seconds by default). If response is received, ‘!’ is displayed. If no response is received, ‘.’ displayed, and the statistics is displayed at the end. For the extension functions of ping ipv6, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

Configuration Examples

The example below 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 example below shows the extension ping ipv6.
Ruijie# ping  ipv6 2000::1  length 1500 ntimes 100 timeout 3 data ffff source
192.168.4.10:
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

traceroute

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

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

Parameter Description

Parameter	Description
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 concrete configuration, refer to the DNS Configuration part.

Configuration Examples The following is two examples of the application bout traceroute, the one is of the smooth network, and the other is the network in which some gateways aren’t connected successfully.

1. When the network is connected smoothly:

```
Ruijie# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36

1     192.168.12.1      0 msec   0 msec   0 msec
2     192.168.9.2       4 msec   4 msec   4 msec
3     192.168.9.1       8 msec   8 msec   4 msec
4      192.168.0.10     4 msec   28 msec  12 msec
5      192.168.9.2      4 msec   4 msec   4 msec
6      202.101.143.154      12 msec  8 msec   24 msec
7      61.154.22.36     12 msec  8 msec   22 msec
```

From above result, it’s clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute 202.108.37.42
  < press Ctrl+C to break >
Tracing the route to 202.108.37.42

1     192.168.12.1      0 msec    0 msec  0 msec
2     192.168.9.2       0 msec    4 msec  4 msec
3     192.168.110.1     16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129      12 msec   28 msec  12 msec
6     61.154.8.17       8 msec    12 msec  16 msec
7     61.154.8.250      12 msec   12 msec  12 msec
```

```
8      218.85.157.222   12 msec   12 msec  12 msec
9       218.85.157.130   16 msec   16 msec  16 msec
10      218.85.157.77    16 msec   48 msec  16 msec
11      202.97.40.65     76 msec   24 msec  24 msec
12      202.97.37.65     32 msec   24 msec  24 msec
13      202.97.38.162    52 msec   52 msec  224 msec
14      202.96.12.38     84 msec   52 msec  52 msec
15      202.106.192.226  88 msec   52 msec  52 msec
16      202.106.192.174      52 msec   52 msec  88 msec
17      210.74.176.158   100 msec  52 msec  84 msec
18      202.108.37.42    48 msec   48 msec  52 msec
The above result clearly shown that the gateways passed by the packets sent
to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent
time are displayed, and gateway 4 fails.
Ruijie# traceroute www.ietf.org

Translating "www.ietf.org"...[OK]
  < press Ctrl+C to break >
Tracing the route to 64.170.98.32

 1      192.168.217.1    0 msec  0 msec  0 msec
 2      10.10.25.1       0 msec  0 msec  0 msec
 3      10.10.24.1       0 msec  0 msec  0 msec
 4      10.10.30.1       10 msec 0 msec  0 msec
 5      218.5.3.254      0 msec  0 msec  0 msec
 6      61.154.8.49      10 msec 0 msec  0 msec
 7      202.109.204.210  0 msec  0 msec  0 msec
 8      202.97.41.69     20 msec 10 msec 20 msec
 9      202.97.34.65     40 msec 40 msec 50 msec
 10     202.97.57.222    50 msec 40 msec 40 msec
 11     219.141.130.122  40 msec 50 msec 40 msec
 12     219.142.11.10    40 msec 50 msec 30 msec
 13     211.157.37.14    50 msec 40 msec 50 msec
 14     222.35.65.1      40 msec 50 msec 40 msec
 15     222.35.65.18     40 msec 40 msec 40 msec
 16     222.35.15.109    50 msec 50 msec 50 msec
 17     *      *      *
 18     64.170.98.32    40 msec 40 msec 40 msec
```

Related Commands

Command	Description

Platform Description

N/A

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
ipv6-address	Specifies an IPv6 address.
number	Specifies the number of probe packets to be sent.
seconds	Specifies the timeout time.
minimum maximum	Specifies the minimum and maximum TTL values.

Defaults

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 concrete configuration, refer to the DNS Configuration part.

Configuration Examples

The following is two examples of the application bout traceroute ipv6, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1       0 msec  0 msec  0 msec
2     3001::1       4 msec  4 msec 4 msec
3     3002::1       8 msec  8 msec  4 msec
4     3004::1       4 msec  28 msec  12 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~4) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# traceroute ipv6 3004::1
 < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1       0 msec  0 msec  0 msec
2     3001::1       4 msec  4 msec 4 msec
3     3002::1       8 msec  8 msec  4 msec
4     * * *
5     3004::1       4 msec  28 msec  12 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 3004::1 (gateways 1~5) and the spent time are displayed, and gateway 4 fails.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

TCP Configuration Commands

ip tcp mss

Use this command to configure the upper limit of 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 MSS value. Range: 68-10000 bytes.

Default Settings

The upper limit is not set by default.

Command mode

Global configuration mode.

Usage guidelines

This command is used to limit the maximum value of MSS for the TCP session 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.

Examples

```
Ruijie(config)# ip tcp mss 1300
```

Related commands

Command	Description
-	-

ip tcp not-send-rst

Use this command to prohibit sending the reset packet when the 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
-	-

Default Settings

The reset packet is sent when the port-unreachable packet is received.

Command mode

Global configuration mode.

Usage guidelines

When the TCP module distributes TCP packets, if the TCP session to which such packets belong cannot be found, a reset packet will be replied to the peer end to terminate the TCP session. The attacker may initiate attacks by sending excess port-unreachable TCP packets. You can use this command to prohibit sending the reset packet when the port-unreachable packet is received.

Examples

```
Ruijie(config)# ip tcp not-send-rst
```

Related commands

Command	Description
-	-

ip tcp path-mtu-discovery

Use this command to enable PMTU(Path Maximum Transmission Unit) 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. Range: 10-30 minutes. Default: 10.
age-timer infinite	No further discovery after discovering PMTU.

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

Based on the 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 the existent TCP connection and is only effective for the TCP connection to be created. This command is valid for both the IPv4 and IPv6 TCP.

According to the RFC1191, after discovering the PMTU, the TCP uses greater MSS to detect the new PMTU at some interval, which is specified by the parameter **age-timer**. If the PMTU discovered is smaller than the MSS negotiated between both ends of the TCP session, the device will be trying to discover the greater PMTU at the specified interval until the PMTU value reaches the MSS or the user stops using this timer. Use the parameter **age-timer infinite** to stop this timer.

Examples

```
Ruijie(config)# ip tcp path-mtu-discovery
```

Related commands

Command	Description
show tcp pmtu	Show the PMTU value for the TCP session.

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. Range: 5-300 seconds; default: 20

Default Settings

20 seconds

Command mode

Global configuration mode.

Usage guidelines

If there is SYN attack in the network, reducing the SYN timeout value can prevent resource consumption, but it takes no effect to the successive SYN attacks. When the device actively request for the connection with the external, reducing the SYN timeout value can shorten the time for the user to wait, such as telnet. For the bad network, the timeout value can be increased properly.

Examples

```
Ruijie(config)# ip tcp syntime-out 10
```

Related commands

Command	Description
-	-

ip tcp window-size

Use this command to change the size of receiving buffer and sending buffer for TCP session. 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	Change the size of receiving buffer and sending buffer for TCP session. Range: 0-65535 bytes; default: 4096.

Default Settings

4096 bytes

Command mode

Global configuration mode.

Usage guidelines

The TCP receiving buffer is utilized to buffer the data received from the peer end. These data will be subsequently read by the application program. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For sessions featuring greater bandwidth ratio and excess data, increasing the size of receiving buffer will provide notable TCP transmission performance. The sending buffer is utilized to buffer the data of application program. Each byte in the buffer has its sequence number, and byte with sequence number acknowledged will be removed from the sending buffer. Increasing the sending buffer will improve the interaction between TCP and application program and thus enhance 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 session.

This command changes both the receiving buffer and sending buffer, and only applies to the newly established session.

Examples

```
Ruijie(config)# ip tcp window-size 16386
```

Related commands

Command	Description
-	-

show tcp connect

Use this command to display basic information about the current TCP sessions.

show tcp connect

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

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
```

The following table lists the field description :

Field	Description
TCB	The control block's location address in the current memory.
Local Address	The local address and port number. The number after the last "." is the port number. For example, "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, "2002::2.23" and "192.168.195.212.23" , "23" is the port number.
State	There are eleven possible states of the current TCP session:

		CLOSED: The session has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packets have been sent out. SYNRCVD: In the three-way handshake phase when the SYN packets have been received. ESTABLISHED: TCP session has been established. FINWAIT1: The local end has sent out 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 out its FIN packet. CLOSING: The local end has sent out 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
-	-

show tcp pmtu

Use this command to display information about TCP PMTU.

show tcp pmtu

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

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
```

The following table lists the field description :

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, "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, “2002::2.23” and “192.168.195.212.23” , “23” is the port number.
PMTU	The PMTU value.

Related commands

Command	Description
ip tcp path-mtu-discovery	Enable the TCP PMTU discovery function.

show tcp port

Use this command to information about the current TCP port.

show tcp port

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

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.
```

The following table lists the field description :

Field	Description
TCB	The control block’s location address in the current memory.
Foreign Address	The remote address
Port	The remote port number
State	There are eleven possible states of the current TCP session: CLOSED: The session has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packets have been sent out. SYNRCVD: In the three-way handshake phase when the SYN packets have been received.

	ESTABLISHED: TCP session has been established. FINWAIT1: The local end has sent out 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 out its FIN packet. CLOSING: The local end has sent out 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
-	-

IPv4 REF Configuration Commands

ip ref broadcast-in-vlan

ip ref broadcast-in-vlan

Parameter Description

Parameter	Description
-	-

Default configuration

None

Command mode

Global configuration mode

Usage guide

Express forwarding obtains the MAC address corresponding to the next hop of the route from the ARP table and then obtain the corresponding physical port from the MAC adders. If no physical port found in the MAC address, how will the chip process the packets matching to this route? Broadcast the packets in the virtual LAN (also called as flooding) or drop the packets? Broadcom chips do not support the flooding, while the Marvell chips do. By default, the chip drops the packets. After enabling the flooding switch with this command, the chip will broadcast the packets in the virtual LAN.

This command takes effect for the routes excluding the routes which have been configured to hardware. Therefore, save the configuration and restart the switch in order to unify all routes.

Configuration examples

```
Ruijie(config)# ip ref broadcast-in-vlan
WARNING: It will take effect after rebooting.Please save configuration and reboot switch.
```

Related commands

Command	Description
-	-

Platform description

N/A

Command history

Version	Description
-	-

ip ref synchronize all

Use this command to synchronize the hardware forwarding table with the software forwarding table. For the Layer3 switches, the hardware and software forwarding tables are often inconsistent because the total number of the routes in the software forwarding table exceeds the capacity of the hardware forwarding table or the hardware hash-bucket collides. For the former, user shall reduce the number of the routes as possible, then execute this command to synchronize the hardware forwarding table with the software forwarding table. Currently, there is no solution to the hardware hash-bucket collision.

ip ref synchronize all

Parameter Description

Parameter	Description
-	-

Default configuration

None

Command mode

Privileged EXEC mode

Usage guide

On condition that the software forwarding table is not consistent with the hardware forwarding table, execute this command to perform the synchronization. The following message is printed to inform users of synchronization finished: “IPv4 express forward reports that synchronization finished”.

Configuration examples

```
Ruijie# ip ref synchronize all
Oct  7 20:09:08 %7: IPv4 express forward reports that
synchronization finished.
```

Related commands

Command	Description
-	-

Platform description

N/A

Command history

Version	Description
-	-

show ip ref

This command is used to display current global statistics of REF, including current routing number, adjacent node number, load balancing table number and weight node number. This command is as follows:

show ip ref

Parameter Description

Parameter	Description
-	-

Default configuration

None

Command mode

Privilege mode

Usage guide

This command can be used to display current packet statistics of REF.

Configuration examples

```
Ruijie# show ip ref
-----------statistic information-----------:
current     routes: 5
alloc weight_nodes: 5
alloc   bal_tables: 0
alloc    adj_nodes: 5
alloc      res_adj: 0
```

Field	Description
routes	Number of routes in the REF table
weight_nodes	Number of the weight nodes.
bal_tables	Number of the load balancing tables
adj_nodes	Number of the adjacent nodes.
res_adj	Number of the registered resolution nodes.

Related commands

Command	Description
-	-

Platform description

N/A

Command history	Version	Description
	-	-

show ip ref adjacency

This command can be used to display a special adjacent node or all the current adjacent nodes. This command is as follows:

show ip ref adjacency [**glean | local |** *ip* **| interface** *interface_type interface_number*]

Parameter Description	Parameter	Description
	glean	Gleans the adjacent nodes.
	local	Local adjacent nodes
	ip	IP of the next hop
	interface_type	Specifies the type of interface
	interface_number	Specifies the number of interface

Default configuration

None

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
adj_type    next_hop       mac          interface
local_adj   0.0.0.0        0000.0000.0000  NULL
glean_adj   0.0.0.0        0000.0000.0000
FastEthernet 1/1
local_adj   0.0.0.0        0000.0000.0000  NULL
glean_adj   0.0.0.0     0000.0000.0000  Loopback 0
forward_adj  192.168.17.1   0000.2004.094f
FastEthernet 1/1
```

Example 2: Display the adjacent information associated with the specified interface.

```
Ruijie# show  ip ref adjacency interface fastEthernet  1/1
adj_type    next_hop       mac          interface
forward_adj  192.168.17.1   0000.2004.094f
FastEthernet 1/1
```

```
Example 3: Display the adjacent node information associated with
the specified IP.
Ruijie# show ip ref adjacency 192.168.17.1
adj_type    next_hop       mac          interface
forward_adj  192.168.17.1   0000.2004.094f
FastEthernet 1/1
```

```
Example 4: Display the gleaned adjacent information.
Ruijie# show ip ref adjacency glean
adj_type    next_hop       mac         interface
glean_adj   0.0.0.0         FastEthernet 0/0
0000.0000.0000
Example 5: Display the local adjacent information.
Ruijie# show ip ref adjacency local
adj_type    next_hop       mac         interface
local_adj   0.0.0.0        0000.0000.0000  NULL
local_adj   0.0.0.0        0000.0000.0000  NULL
```

Field	Description
adi_type	Adjacent type
next_hop	Address of next hop
mac	MAC address (0 means invalid)
interface	Interface

Related commands

Command	Description
show ip ref route	Displays all routing information in the current REF module.

Platform description

N/A

Command history

Version	Description
-	-

show ip ref route

This command can be used to display all the routing information on the current REF module. This command is as follows:

show ip ref route [**default** | *ip mask*]

Parameter Description

Parameter	Description
default	Specifies default route.
ip	Specifies the destination IP address of route.
mask	Specifies the route mask.

Default configuration

None

Command mode

Privileged EXEC mode

Usage guide

Display the related routing information in 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       adj-id next-hop         weight     interface
    224.0.0.0     224.0.0.0     1      0.0.0.0       1
192.168.52.0      255.255.255.0    11     0.0.0.0       1
FastEthernet 0/0
192.168.52.255    255.255.255.255 1    0.0.0.0       1
```

```
192.168.52.68     255.255.255.255 1    0.0.0.0       1
192.168.52.58     255.255.255.255   12  192.168.52.58 1
FastEthernet 0/0
20.0.0.0          255.255.255.0     10     0.0.0.0          1
   FastEthernet 0/1.1
20.0.0.255    255.255.255.255   1      0.0.0.0          1
20.0.0.3      255.255.255.255   1      0.0.0.0       1
```

Example 2: Display all the default routing information in the REF table.

```
Ruijie# show ip ref route default
IP/MASK        s/res   w   adj_type    next_hop
mac           interface
*0.0.0.0/0              1/1      1   forward_adj   192.168.17.1
0000.2004.094f  FastEthernet 1/1
```

Example 3: Display all the routing information matching the IP/MASK in the REF table.

```
Ruijie# show ip ref route 192.168.17.0 255.255.255.0
IP/MASK        s/res   w   adj_type    next_hop
mac           interface
192.168.17.0/24    1/1    1  glean_adj   0.0.0.0 0000.0000.0000
FastEthernet 1/1
```

Field	Description
ip	Destination IP address
mask	Mask
s	Associated route number.
res	Resolution route number.
weight	Routing weight
adj-type	Adjacent type
next-hop	Address of next hop
mac	MAC address (0 means invalid)
interface	Egress

Related commands

Command	Description
show ip ref exact-route	Displays the accurate REF forwarding path of a IP packet.

Platform description

N/A

Command history

Version	Description
-	-

IP Routing Configuration Commands

1. IP Routing Configuration Commands

IP Routing Configuration Commands

ip default-network

Use this command to configure the default network globally. Use the **no** form of this command to remove the setting.

ip default-network *network*

no ip default-network *network*

Parameter description

Parameter	**Description**
network	Default network

Default configuration

0.0.0.0/0

Command mode

Global configuration mode.

Usage guidelines

The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network.

The default network always starts with an asterisk (“*”), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

Examples

The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.

```
ip route 192.168.100.0 255.255.255.0 serial 0/1
ip default-network 192.168.100.0
```

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
ip default-network 200.200.200.0
```

Related commands

Command	Description
show ip route	Show the routing table.

ip route

Use this command to configure a static route. Use the **no** form of this command to remove the configured route.

ip route *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent]** [**disable** | **enable**]

no ip route *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent]** [**disable** | **enable**]

Parameter description

Parameter	Description
network	Network address of the destination

net-mask	Mask of the destination
ip-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The management distance of the static route
tag	(Optional) The tag of the static route
permanent	(Optional) Permanent rotue ID
disable/enable	(Optional) Disablement or enablement ID of the static route

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

The default management distance of the static route is 1. Setting the management distance allows the learnt dynamic route to overwrite the static route. Setting the management distance of the static route can enable route backup, which is called floating route in this case.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it.

When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, ip route 0.0.0.0 0.0.0.0 Fastethernet 0/0. In this case, the switch may consider that all unknown destination networks are directly connected to the Fastethernet 0/0. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

Note The IS2700G series products support up to 32 IPv4 static routes.

Note The IPv4 static route supports only the default route with the mask being 0, and the host route with the mask being 32.

Examples

The following example configures a default route whose next hop is 192.168.12.1.

```
Ruijie(config)# ip route 0.0.0.0 0.0.0.0 192.168.12.1
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 172.16.100.1/32.

```
Ruijie(config)# ip route 172.16.100.1 255.255.255.255 fastethernet 0/0
192.168.12.1
```

Related commands

N/A

ip routing

Use this command to enable IPv4 routing. Use the **no** form of this command to disable the function.

ip routing

no ip routing

Default configuration

Enabled

Command mode

Global configuration mode.

Usage guidelines

IPv4 static routes will become ineffective if the IPv4 routing is disabled.

Note

The IS2700G series products support only the IPv4 or IPv6 static routes, and IPv4 or IPv6 directly connected route.

Note

Configure the static route to obtain the IPv4 or IPv6 static route.

Note

Configure the IP address of the SVI to obtain the IPv4 or IPv6 directly connected route.

Examples

The following example disables IP routing

```
no ip routing
```

Related commands

N/A

Platform description

N/A

ip static route-limit

Use this command to set the upper limit of the static route. 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

Parameter description

Parameter	Description
number	Upper limit of static routes, range: 1 to 32.

Default configuration

-

Command mode

Global configuration mode.

Usage guidelines

The goal is to control the number of static routes.

Note

The IS2700G series products support up to 32 IPv4 static routes.

Examples

The following example sets the upper limit of the static routes to 10 and then restores the setting to the default value.

```
Ruijie(config)# ip static route-limit 10
Ruijie(config)# no ip static route-limit
```

Related commands

N/A

Platform description

N/A

ipv6 route

Use this command to configure an IPv6 static route. Use the **no** form of this command to delete the configured route.

ipv6 route *ipv6-prefix / prefix-length* { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*]

Parameter description

Parameter	Description
ipv6-prefix	IPv6 prefix, which must comply with the IP address form defined in RFC4291.
prefix-length	Length of the IPv6 prefix. The symbol of “ / ” must be added in front of the prefix.
ipv6-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The management distance of the static route

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

The default management distance of the static route is 1. Setting the management distance allows the learnt dynamic route to overwrite the static route. Setting the management distance of the static route can enable route backup, which is called floating route in this case.

Note

The IS2700G series products support up to 16 IPv6 static routes.

Note The IPv6 static route supports only the default route with the mask being 0, and the host route with the mask being 128.

Examples

The following example configures a default route whose next hop is 2002::2.

```
Ruijie(config)#ipv6 route 0::/0 2002::2
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 2001::/128.

```
Ruijie(config)#ipv6 route 2001::1/128 fastethernet 0/0 2002::2
```

Related commands

Command	Description
show ipv6 route	Show IPv6 routing table .

Platform description N/A

ipv6 static route-limit

Use this command to set the upper limit of the static route. 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 limit of static routes, range: 1 to 16.

Default configuration -

Command mode Global configuration mode.

Usage guidelines

The goal is to control the number of static routes.

Note The IS2700G series products support up to 16 IPv6 static routes.

Examples

The following example sets the upper threshold of the ipv6 static routes to 10 and then restores the setting to the default value.

```
Ruijie# ipv6 static route-limit 10
Ruijie# no ipv6 static route-limit
```

Related commands

Command	Description
ipv6 route	Configure the IPv6 static route.
show ipv6 route	Show IPv6 routing table

Platform description

N/A

ipv6 unicast-routing

Use this command to enable the IPv6 routing. Use the **no** form of this command to disable this function.

ipv6 unicast-routing

no ipv6 unicast-routing

Parameter description

None

Default configuration

Enabled

Command mode

Global configuration mode

Usage guidelines

IPv6 static routes will become ineffective if the IPv6 routing is disabled.

Note

The IS2700G series products support only the IPv4 or IPv6 static routes, and IPv4 or IPv6 directly connected route.

Note

Configure the static route to obtain the IPv4 or IPv6 static route.

Note

Configure the IP address of the SVI to obtain the IPv4 or IPv6 directly connected route.

Examples

The example disables the IPv6 routing

```
Ruijie# no ipv6 unicast-routing
```

Related commands

Command	Description
ipv6 route	Configure the IPv6 static route
show ipv6 route	Show the IPv6 routing table

Platform description

N/A

show ip route

Use the command to show the IPv4 routing table.

show ip route [*network* [*mask*] | **count** | **summary**]

Parameter description

Parameter	Description
network	(Optional) Show the route information to the network.
mask	(Optional)Show the route information to the network of this mask.
count	(Optional)Show the number of existent routes. (for the ECMP/WCMP route, show one route)
summary	(Optional) Show statistics of the routing table.

Default configuration

All routes are displayed by default.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

N/A

Examples

```
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 default

Gateway of last resort is no set
S 20.0.0.0/8 is directly connected, VLAN 1
S 22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R 40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B 50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C 192.1.1.0/24 is directly connected, VLAN 1
C 192.1.1.254/32 is local host.
```

Field	Description

O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route ia: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Manage metric
Via 20.0.0.1	Next hop IP address.
VLAN 1	Forwarding interface of next hop

```
Ruijie# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
*192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Field	Description
Routing Descriptor Blocks	Next hop IP address, source, update time, forwarding interface, source routing protocol and type of route information

The following is the showing result 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 is the showing result 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

Ruijie# show ip route count
--------- route info ----------
the num of active route: 5

Ruijie# show ip route weight
------------[distance/metric/weight]-----------
S 23.0.0.0/8 [1/0/2] via 192.1.1.20
S 172.0.0.0/16 [1/0/4] via 192.0.0.1
```

The following is the showing result of the show ip reroute 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

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
```

show ipv6 route

Use the command to view the configuration of the IPv6 routing table.

show ipv6 route [[*network/prefix-length*] | **summary**]

Parameter description

Parameter	Description
network/prefix-length	(Optional) Show the route information to the network.
summary	(Optional)Show the classified statistics of the number of ipv6 routes.

Default configuration

All routes are displayed by default.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

This command can show route information flexibly.

Examples

The following is the output of this command:

```
Ruijie(config)# show ipv6 route
IPv6 routing table -  Default - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, 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 host
```

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route ia: IS-IS area internal route
20::/64	Network address and mask of the destination network
[1/0]	Manage metric
Via 10::4	Next hop IP address.
00:00:06	Survival time of the protocol route
VLAN 1	Forwarding interface of next hop

Related commands

Command	Description
ipv6 route	Configure the ipv6 static route.

Platform description N/A

Multicast Configuration Commands

1. IGMP Snooping Configuration Commands

2. MLD Snooping Configuration Commands

3. Multicast Forwarding Control Configuration Commands

IGMP Snooping Configuration Commands

debug igmp-snp

Use the following commands to turn on igmp service debug switch. The **no** form of this command closes debug switch.

debug igmp-snp

debug igmp-snp event

debug igmp-snp packet

debug igmp-snp msf

debug igmp-snp warning

undebug igmp-snp

undebug igmp-snp event

undebug igmp-snp packet

undebug igmp-snp msf

undebug igmp-snp warning

Parameter description

Parameter	Description
none	Show all debug information of IGMP Snooping.
event	Show the debug information of IGMP Snooping event.
packet	Show the debug information of IGMP Snooping packet.
msf	Show the debug information exchanged between the IGMP Snooping and multicast.
warning	Show all debug information of IGMP Snooping warning.

Command mode Privileged EXEC mode.

deny

To deny the forwarding of the multicast streams in the range specified by the profile, execute the deny configuration command in the profile configuration mode.

Parameter description N/A

Default The forwarding of the multicast streams in the range specified by the profile is denied.

Command mode Profile configuration mode.

Usage guidelines First, configure the multicast range using the range command in the profile configuration mode.

In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Examples

The following is an example of deny the forwarding of the multicast stream 224.2.2.2 to 224.2.2.244:

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# deny
```

Related commands

Command	Description
ip igmp profile	Create a profile.
range	Configure the multicast address range.

ip igmp profile

Use this command to select a profile and enter the IGMP profile configuration mode.

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

Parameter description

Parameter	Description
profile-number	Profile number, in the range from 1 to 1024

Default N/A.

Command mode Global configuration mode.

Usage guidelines The profile must be applied to the specified interface in order to make the profile take effect.

Examples

The following is an example of creating a profile numbered 1 and entering the profile configuration mode.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)#
```

Related commands

Command	Description
range	Configure the multicast address range.

ip igmp snooping dyn-mr-aging-time

To configure the aging time of the routing interface that the switch learns dynamically, execute the **ip igmp snooping dyn-mr-aging-time** command .

ip igmp snooping dyn-mr-aging-time *time*

no ip igmp snooping dyn-mr-aging-time

Parameter description

Parameter	Description
time	Aging time of the routing interface that the switch learns dynamically

Default configuration

300s.

Command mode

Global configuration mode.

Usage guidelines

When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.

Examples

Set the aging time of the routing interface that the switch learns dynamically to 100 s:

```
Ruijie(config)# ip igmp snooping dyn-mr-aging-time 100
```

Related commands

Command	Function
ip igmp snooping	Enable IGMP Snooping.

ip igmp snooping fast-leave enable

To enable the fast leave function, execute the **ip igmp snooping fast-leave enable** command in the global configuration mode. The **no** form of this command is used to disable the function.

ip igmp snooping fast-leave enable

no ip igmp snooping fast-leave enable

Parameter description

Parameter	Description
N/A	

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message.

Subsequently, when the system receives a specific group query packet, the system does not forward it to the corresponding interface. Leave packets include IGMPv2 leave packets and IGMPv3 report packets of the include type without source addresses. The fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.

Examples

The following example shows how to enable the fast leave function on the switch:

```
Ruijie(config)# ip igmp snooping fast-leave
```

Related commands

Command	Function
N/A	

ip igmp snooping filter

To configure a port to receive a specific set of multicast streams, execute the **ip igmp snooping filter** command in the interface configuration mode to associate the port to a specific profile. The **no** form of this command is used to delete the associated profile.

ip igmp snooping filter *profile-number*

no ip igmp snooping filter *profile-number*

Parameter description

Parameter	Description
profile-number	Profile number, range: 1 to 1024

Default N/A.

Command mode Global configuration mode or interface configuration mode.

Usage guidelines A specific profile must be created before association.

Examples

The following example demonstrates how to associate profile 1 to a megabit port 0/1:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

Related commands

Command	Description
ip igmp profile	Create a profile.

ip igmp snooping host-aging-time

Use this command to configure the aging time of IGMP dynamic ports. The **no** form of this command is used to restore the default aging time.

ip igmp snooping host-aging-time *seconds*

no ip igmp snooping host-aging-time

Parameter description

Parameter	Description
seconds	Aging time. The unit is second. The value ranges from 1 to 65,535. The default value is 260.

Default 260

Command mode Global configuration mode

Usage guideline

The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group.

When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by **host-aging-time**. If the timer expires, the system determines that there is no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the **ip igmp snooping host-aging-time** command is executed, the aging time will be determined by **host-aging-time**. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.

Example

The following example shows how to set the aging time to 30 seconds:

```
Ruijie(config)# ip igmp snooping host-aging-time 30
```

Related command

Command	Description
-	-

Platform description

-

ip igmp snooping limit-ipmc

To add a multicast source IP address check entry, execute the **ip igmp snooping limit-ipmc** command in the global configuration mode. The **no** form of this command is used to delete a source IP checklist entry.

ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

no ip igmp snooping limit-ipmc vlan *vid* **address** *gaddress* **server** *saddress*

Parameter description

Parameter	Description
vid	VLAN ID of the source IP address check entry
gaddress	Multicast address
Saddress	Multicast source IP address (multicast server)

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

The source IP address check function must be enabled before an entry can be added.

Examples

The following is an example of adding an entry to the multicast source IP address check table.

```
Ruijie(config)# ip igmp snooping limit-ipmc vlan 1 address 224.0.0.1 server
192.168.4.243
```

Related commands

Command	Description
ip igmp snooping source-check default-server	Configure a default source IP address while enabling the IP check function.

ip igmp snooping max-groups

To configure the maximum number of groups that can be added dynamically to this interface, execute the **ip igmp snooping max-groups** command in the interface configuration mode. The **no** form of this command is used to remove the configuration.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

Parameter description

Parameter	Description
number	The parameter ranges 0 to 1024.

Default N/A.

Command mode Interface configuration mode.

Usage guidelines If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this interface is beyond the range.

Examples The following example shows how to configure the maximum number of multicast groups to 100 on the megabit interface 0/1:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip igmp snooping max-group 100
```

Related commands

Command	Description
ip igmp snooping filter	Filter multicast groups that pass through a port.

ip igmp snooping mrouter learn pim-dvmrp

To configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface, execute the **ip igmp snooping mrouter learn** command in the global configuration mode. The **no** form of this command is used to disable the dynamic learning.

ip igmp snooping vlan *vid* **mrouter learn pim-dvmrp**

no ip igmp snooping vlan *vid* **mrouter learn pim-dvmrp**

Default Enabled

Command Global configuration mode.

mode

Parameter description

Parameter	Description
vid	VLAN ID

Usage guidelines

Routing interface is a port through which a multicast device (with IGMP Snooping enabled) is directly connected to a multicast neighbouring device (with multicast routing protocols enabled).

By default, the dynamic routing interface learning function is enabled. You can use the no form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled.

Examples

The following example demonstrates how to enable the dynamic routing interface learning function on the equipment:

```
Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp
Ruijie(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

Related commands

Command	Description
ip igmp snooping vlan mrouter learn pim-dvmrp	Enable the dynamic routing interface learning function on the multicast routing port.

ip igmp snooping preview

Allow the user to preview the specific multicast streams when the user doesn't have access to such multicast streams. Use **no** form of this command to disable multicast preview.

ip igmp snooping preview *profile-number*

no ip igmp snooping preview

Parameter description

Parameter	Description
profile-number	Profile number (1-1024)

Default No default value

Command mode Global configuration mode.

Usage guidelines

Apply the IGMP Profile to a multicast preview function. When the user doesn't have access to the multicast streams (namely the user might be filtered by IGMP Snooping filter), it can allow the user to preview partial contents. This function shall be used in conjunction with IGMP Snooping filter or multicast control in order to realize effective multicast preview.

Examples

The following example associates the profile 1 to the 100M port 0/1 and associates multicast preview with profile 2:

```
Ruijie(config)# ip igmp snooping preview 2
Ruijie(config-if)# int fa 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

Related commands

Command	Description
ip igmp profile	Create a profile

Platform description

N/A

ip igmp snooping preview interval

Use this command to configure the interval that allows the user to preview the specific multicast streams when the user doesn't have access to such multicast streams. Use **no** form of this command to restore the preview interval to the default value.

ip igmp snooping preview interval *num*

no ip igmp snooping preview interval

Parameter description

Parameter	Description
num	Preview interval (1-300); default: 60 seconds.

Default

The default value is 60 seconds.

Command mode

Global configuration mode.

Usage guidelines

NA

Examples

The following example sets the multicast preview interval as 100 seconds on the 100M port of 0/1:

```
Ruijie(config)# ip igmp snooping preview interval 100
```

Related commands

Command	Description
ip igmp snooping preview	Enable the multicast preview.

Platform description

N/A

ip igmp snooping querier

To enable the IGMP querier function, execute "**ip igmp snooping querier**" global configuration command. Use **no** form of this command to disable IGMP querier in all VLANs and disable the global configurations.

ip igmp snooping [**vlan** *vid*] **querier**

no ip igmp snooping [**vlan** *vid*] **querier**

Parameter description

Parameter	Description
vlan *vid*	VLAN ID

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to effect this command.

If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.

Examples

The following example enables the IGMP querier function on the device:

```
Ruijie(config)# ip igmp snooping querier
```

Related commands

Command	Description
N/A	N/A

Platform description

N/A

ip igmp snooping querier address

To enable the IGMP querier, you also need to specify a source IP address for query packets. Execute the global configuration command of "**ip igmp snooping querier address**". Use **no** form of this command to remove the source IP address configured.

ip igmp snooping [**vlan** *vid*] **querier address** *a.b.c.d*

no ip igmp snooping [**vlan** *vid*] **querier address**

Parameter description

Parameter	Description
a.b.c.d	Source IP address of the query packets.
vlan *vid*	VLAN ID

Default

No source IP address is specified

Command mode

Global configuration mode.

Usage

After enabling IGMP querier, you also need to configure a source IP address for query packets, so

guidelines

that the device can send packets normally.

If no source IP address is specified in the VLAN needing to send packets, the device will verify whether the source IP address is specified globally. The device can only send query packets after finding the source IP configured, or else the querier function won't take effect.

If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.

Examples

The following example specifies the source IP of query packets on the device:

```
Ruijie(config)# ip igmp snooping querier address 1.1.1.1
```

Related commands

Command	Description
ip igmp snooping vlan querier address	Enable the source IP check in VLAN

Platform description

N/A

ip igmp snooping querier max-response-time

To configure the maximum response time advertised in query packets, execute the global configuration command of "**ip igmp snooping querier max-response-time**". Use **no** form of this command to restore to the default value.

ip igmp snooping [**vlan** *vid*] **querier max-response-time** *seconds*
no ip igmp snooping [**vlan** *vid*] **querier max-response-time**

Parameter description

Parameter	Description
seconds	Maximum response time (1-25); unit: second; default: 10
vlan *vid*	VLAN ID

Default

Default value

Command mode

Global configuration mode.

Usage guidelines

Configure this command to specify the maximum response time to query packets.

By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.

Examples

The following example specifies the maximum response time to query packets on the device:

```
Ruijie(config)# ip igmp snooping querier max-response-time 15
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

ip igmp snooping querier query-interval

To specify the interval for IGMP querier to send query packets, execute the global configuration command of "**ip igmp snooping querier query-interval**". Use **no** form of this command to restore the query interval to the default value.

ip igmp snooping [**vlan** *vid*] **querier query-interval** *seconds*

no ip igmp snooping [**vlan** *vid*] **querier query-interval**

Parameter description

Parameter	Description
seconds	Query interval (1-18000); unit: second; default: 60 seconds
vlan *vid*	VLAN ID

Default Default value

Command mode Global configuration mode.

Usage guidelines

After globally enabling IGMP querier, the timer will be enabled for sending query packets periodically. The aging time of the timer is the query interval. Configure this command to change the query interval.

If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Examples

The following example configures the query interval on the device:

```
Ruijie(config)# ip igmp snooping querier query-interval 100
```

Related commands

Command	Description
N/A	N/A

Platform description N/A

ip igmp snooping querier timer expiry

To specify the expiration timer for non-querier, execute the global configuration command of "**ip igmp snooping querier timer expiry**". Use **no** form of this command to restore to the default value.

ip igmp snooping [**vlan** *vid*] **querier timer expiry** *seconds*

no ip igmp snooping [**vlan** *vid*] **querier timer expiry**

Parameter

Parameter	Description

description

seconds	Non-querier expiration timer (60-300); unit: second; default: 125 seconds
vlan *vid*	VLAN ID

Default

Default value

Command mode

Global configuration mode.

Usage guidelines

After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier.

If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Examples

The following example configures the non-querier expiration timer on the device:

```
Ruijie(config)# ip igmp snooping querier timer expiry 60
```

Related commands

Command	Description
ip igmp snooping vlan querier timer expiry	Configure querier expiration timer in VLAN

Platform description

N/A

ip igmp snooping querier version

Currently, the IGMP Snooping querier supports IGMPv1 and IGMPv2. To specify the version, execute the global configuration command of "**ip igmp snooping querier version**". Use **no** form of this command to restore to the default setting.

ip igmp snooping [**vlan** *vid*] **querier version** { **1** | **2** }

no ip igmp snooping [**vlan** *vid*] **querier version**

Parameter description

Parameter	Description
1	IGMPv1
2	IGMPv2
vlan *vid*	VLAN ID

Default

IGMPv2

Command mode

Global configuration mode.

Usage guidelines

If the IGMP querier version number has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

Examples

The following example configures IGMP querier version on the device:

```
Ruijie(config)# ip igmp snooping querier version 1
```

Related commands

Command	Description
-	-

Platform description

N/A

ip igmp snooping query-max-response-time

This command specifies the time for the switch to wait for the member join message after receiving the **query** message. If the switch does not receive the member join message within the specified time, it considers that the member has left and then deletes the member.

ip igmp snooping query-max-response-time *time*

no ip igmp snooping query-max-resposne-time

Parameter description

Parameter	Description
time	The aging time of the routing inerface that the switch learns dynamically. Range: 1 to 65535

Default configuration

10s.

Command mode

Global configuration mode.

Usage guidelines

You can specify the time for the switch to wait for the member join message after receiving the query message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member. This command lets you adjust the waiting time after receiving the query message. This command takes effect only after the switch receives the next member join message. This command does not change the current wait time.

Examples

Set the aging time of the routing interface that the switch learns dynamically to 100s.

```
Ruijie(config)# ip igmp snooping query-max-response-time 100
```

Related commands

Command	Function
ip igmp snooping	Configure a multicast routing interface.

ip igmp snooping source-check default-server

The source IP address check is used to permit one or several IPMC flows from the server of the specified IP address.

To configure the source IP address check function of IGMP Snooping, execute the **ip igmp snooping source-check default-server** command in the global configuration mode. The **no** form of this command is used to disable the source IP address check function.

ip igmp snooping source-check default-server *address*

no ip igmp snooping souce-check

Parameter description

Parameter	Description
address	Default multicast source IP address (IP address of the default multicast server)

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

The source IP address check function takes effect globally. Once it is enabled, only the IPMC streams from the specified IP address are permitted. The device allows users to configure the source IP address of all IPMC streams, called default multicast server. The default server must be set as long as the source IP address check function is enabled.

Examples

The following example shows how to enable the multicast source IP address check function and configure a default source IP address.

```
Ruijie(config)# ip igmp snooping source-check default-server 192.168.4.243
```

Related commands

Command	Description
N/A	N/A

ip igmp snooping suppression enable

To enable IGMP Snooping suppression, execute the **ip igmp snooping suppression enable** command in the global configuration mode.The **no** form of this command is used to disable IGMP Snooping suppression..

ip igmp snooping suppression enable

no ip igmp snooping suppression enable

Parameter description

N/A.

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

After you execute this command to enable the suppression function, the switch begins to suppress the IGMP v1/v2 report messages.

Examples

The following example shows how to enable IGMP Snooping suppression on the device:

```
Ruijie(config)# ip igmp snooping suppression
```

Related commands

N/A

ip igmp snooping vlan

Use this command to enable the IGMP Snooping on the specified vlan and enter the ivgl mode. The **no** form of this command is used to disable the IGMP Snooping.

ip igmp snooping vlan *vid*

no ip igmp snooping vlan *vid*

Parameter description

Parameter	Description
vid	VLAN ID, range: 1 to 4094

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

Use this command to enable or disable the IGMP Snooping on the specified vlan.

Caution

The pim snooping on the specified vlan works only when the IGMP Snooping configured. when disabling the IGMP Snooping on the vlan with the pim snooping configured, it prompts to disable the pim snooping first and this execution fails.

Examples

The following example enables the IGMP Snooping on the vlan2.

```
Ruijie(config)# ip igmp snooping vlan 2
```

Related commands

Command	Description
ip igmp snooping	Enable the IGMP Snooping.

ip igmp snooping vlan mrouter interface

Routing interface is a port through which a multicast device is directly connected to a multicast neighbouring device. To configure a multicast routing interface, execute the **ip igmp snooping vlan mrouter interface** command in the global configuration mode. The **no** form of this command is used to delete a routing interface.

ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*

no ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*

Parameter description

Parameter	Description
vid	VLAN ID
interface-type ***interface-number***	Interface name

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.

Examples

The following example demonstrates how to configure a multicast routing interface on the equipment:

```
Ruijie(config)# ip igmp snooping vlan 1 mrout erinterface fastEthernet 0/1
```

Related commands

Command	Description
N/A	N/A

ip igmp snooping vlan static interface

Once IGMP Snooping is enabled, a port can receive a certain multicast frame without being afftected by various IGMP messges by executing the **ip igmp snooping vlan static interface** command in the global configuration mode. The **no** form of this command is used to delete a static configuration.

ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

no ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

Parameter description

Parameter	Description
vid	VLAN ID
group-address	Multicast IP address
interface-type interface-number	Interface name

Default

N/A.

Command

Global configuration mode.

mode

Usage guidelines

Multiple multicast IP addresses can be configured for an interface.

Examples

The following example demonstrates how to configure a static multicast address on a port:

```
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface
GigabitEthernet 0/1
```

Related commands

Command	Description
ip igmp snooping vlan mdevice interface	Configure a multicast routing interface

permit

To permit the forwarding of the multicast streams in the range specified by the profile, execute the **permit** command in the profile configuration mode. In this way, the interface associated with this profile will forward the specified multicast stream only.

permit

Parameter description

N/A

Default

The forwarding of the multicast streams in the range specified by the profile is denied.

Command mode

Profile configuration mode.

Usage guidelines

First, configure the multicast range using the range command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration to take effective.

Examples

The following is an example of allowing the forwarding of the multicast stream 224.2.2.2 to 224.2.2.244:

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# permit
```

Related commands

Command	**Description**
ip igmp profile	Create a profile.
range	Configure the multicast address range.

range

To specify the range of multicast streams, execute the **range** command in the profile configuration mode. You can specify either a single multicast address or a range of multicast addresses. Use the **no** form of the command to remove the specified multicast IP address.

range *low-ip-address* [*high-ip-address*]

no range *low-ip-address* [*high-ip-address*]

Parameter description

Parameter	Description
low-ip-address	Start address of a range
high-ip-address	End address of a range

Default

N/A.

Command mode

Profile configuration mode.

Usage guidelines

You can specify a behavior after configuring the address range, for example deny by default. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

Examples

The following is an example of creating a profile whose multicast stream is in the range 224.2.2.2 to 224.2.2.244:

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
```

Related commands

Command	Description
ip igmp profile	Create a profile.
deny	Deny the forwarding of the multicast streams in the range specified by the profile.
permit	Permit the forwarding of the multicast streams in the range specified by the profile.

show ip igmp profile

Use this command to show the profile information.

show ip igmp profile

show ip igmp profile *profile-number*

Parameter description

Parameter	Description
none	Show configuration information of all profiles.
profile-number	Show configuration information of the designated profile. Profile

	number range: 1 to 1024

Command mode

Privileged EXEC mode.

Examples

```
Ruijie(config-if)# show ip igmp profile
Profile 1
Permit
range 224.0.1.0, 239.255.255.255
```

show ip igmp snooping

Use this command to show related information of IGMP Snooping.

show ip igmp snooping [**gda-table** | **interfaces** | **mrouter**| **statistics** [**vlan** *vid*] | **vlan** *vid*]

Parameter description

Parameter	Description
none	Show the function configuration of IGMP Snooping.
gda-table	Show multicast forwarding rule table.
interfaces	Show the configuration of IGMP Snooping filtering
mrouter	Show interface configuration of multicast device.
statistics	Show the IGMP Snooping statistics.
vlan *vid*	

Command mode

Privileged EXEC mode.

Examples

The following example demonstrates how to process 100 multicast group on the interface fa0/1:

```
Ruijie(config-if)# ip igmp snooping gda-table
Abbr:M - mrouter
D – dynamic
S – static
VLAN Address Member ports
-------------------------------------------
1 233.3.3.3 Gi0/2(S)
2 234.4.4.4 Gi0/11(S)
1 233.4.4.4 Ag2(S)
```

MLD Snooping Configuration Commands

clear ipv6 mld snooping gda-table

Use this command to clear the forwarding table information learned dynamically.

clear ipv6 mld snooping gda-table

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to clear the forwarding table information learned dynamically.

Configuration Examples The following example shows how to clear the forwarding table information learned dynamically:

```
Ruijie# clear ipv6 mld snooping gda-table
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

debug mld-snp

Use this command to enable the mld service debugging switch.

debug mld-snp [**event** | **packet** | **msf** | **warning**]

undebug mld-snp [**event** | **packet** | **msf** | **warning**]

Parameter Description

Parameter	Description
event	Turn on event debugging.
packet	Turn on packet debugging.
msf	Turn on multicast exchange debugging.
warning	Turn on warning debugging.

Defaults N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to enable the mld service debugging switch.

Configuration Examples

```
Ruijie# debug mld-snp
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

deny

Use this command to prevent the multicast flow profile within the specified range from being forwarded in the profile configuration mode.

deny

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default profile action is deny.

Command Mode

Profile configuration mode.

Usage Guide

Before configuring this command, use the **range** command to set the multicast range first.

Configuration Examples

The following example shows how to prevent the multicast flow profile within the range of FF77::1 to FF77::100 from being forwarded:

```
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)# range FF77::1 FF77::100
Ruijie(config-profile)# deny
```

Related Commands

Command	Description
ipv6 mld profile	Create one profile.
range	Set the multicast address range.
permit	Set the profile action permit.

Platform Description N/A

ipv6 mld profile

The MLD profile is used to set a series of the group filter. Before entering the profile mode, a profile must be configured in the global configuration mode. This is a mode navigation command. You can choose the profile-number and enter the mld profile configuration mode.

ipv6 mld profile *profile-number*

no ipv6 mld profile *profile-number*

Parameter Description

Parameter	Description
profile-number	Set the profile number. The valid range is 1-1024.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide MLD Profile is the group filter for the usage of the "multicast address range in the SVGL mode", "multicast data filtering range of the route interface", "MLD Filtering range". To this end, to make the profile effective, the profile and the specific function shall be associated.

Configuration Examples The following example shows how the profile 1 enter the profile configuration mode:

```
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)#
```

Related Commands

Command	Description
range	Set the profile multicast address range.
deny	Set the profile action deny.
permit	Set the profile action permit.

Platform Description N/A

ipv6 mld snooping

Use this command to enable MLD Snooping IVGL mode . Use the **no** form of this command to disable MLD Snooping.

ipv6 mld snooping

no ipv6 mld snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command Mode Global configuration mode.

Usage Guide In this mode, the multicast flow between the VLANs are independent. The host can only request for receiving the multicast flow from the route port in the same VLAN. When receiving the multicast flow from any VLAN, the switch forwards them to the member port in the same VLAN.

Configuration Examples The following example shows how to enable MLD Snooping IVGL mode:

```
Ruijie(config)# ipv6 mld snooping
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld snooping dyn-mr-aging-time

Use this command to set the aging time of the dynamic multicast route port. Use the no form of this command to restore it to the default value.

ipv6 mld snooping dyn-mr-aging-time *time*

no ipv6 mld snooping dyn-mr-aging-time

Parameter Description

Parameter	Description
time	Set the aging time of the dynamic multicast route port, in seconds. The valid range is 1-3600.

Defaults 300s.

Command Mode Global configuration mode.

Usage Guide The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the Ipv6 PIM Hello packets within the aging timeout on this interface.

Configuration Examples

The following example shows how to set the aging time of the dynamic multicast route port as 100s:

```
Ruijie(config)# ipv6 mld snooping dyn-mr-aging-time 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 mld snooping fast-leave enable

Use this command to enable the MLD Snooping fast-leave in the global configuration mode. Use the **no** form of this command to disable this function.

ipv6 mld snooping fast-leave enable

no ipv6 mld snooping fast-leave enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

The interface fast leave is that when IPv6 MLD Leave packets sent from the host are received on an interface, the interface is removed form the outgoing interface list of the corresponding forwarding entry. Then, the switch will not forward the received IPv6 MLD specific group query packets to the interface. If there is only one receiver connected with the interface, enable the interface fast leave function to save the bandwidth and resources.

Configuration Examples

The following example shows how to enable MLD Snooping fast-leave:

```
Ruijie(config-if)# ipv6 mld snooping fast-leave
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 mld snooping filter

Use this command to filter the specific multicast flow in the interface configuration mode. Use the **no** form of this command to delete the associated profile.

ipv6 mld snooping filter *profile-number*

no ipv6 mld snooping filter *profile-number*

Parameter Description

Parameter	Description
profile-number	Set the profile number. Profile number range: 1 to 1024.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide You can configure an MLD Profile on an interface. If the MLD Report packets are received on the interface, the layer-2 device will determine whether the multicast address to be joined the interface is within the allowed range of the MLD Profile. The specified profile must be created before using this command.

Configuration Examples The following example shows how to associate profile1 with the interface fastEthernet 0/1:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 mld snooping filter 1
```

Related Commands

Command	Description
ipv6 mld profile	Create a profile.

Platform Description N/A

ipv6 mld snooping max-groups

Use this command to set the maximum group allowed to join the interface dynamically in the interface configuration mode. Use the **no** form of this command to cancel the limit.

ipv6 mld snooping max-groups *number*

no ipv6 mld snooping max-groups

Parameter Description

Parameter	Description
number	The valid range is 0-1024.

Defaults 1024

Command Mode

Interface configuration mode.

Usage Guide

With this command configured, when the group number exceeds the specified range on the interface, the switch will not receive and deal with the MLD Report packets.

Configuration Examples

The following example shows how to set the maximum 100 multicast group on the interface fastEthernet 0/1:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 mld snooping max-group 100
```

Related Commands

Command	Description
ipv6 mld snooping filter	Filter the multicast group on the interface.

Platform Description

N/A

ipv6 mld snooping query-max-response-time

Use this command to set t the maximum response time of the MLD general query packet. Use the **no** form of this command to restore it to the default value.

ipv6 mld snooping query-max-response-time *time*

no ipv6 mld snooping query-max-response-time

Parameter Description

Parameter	Description
time	Set the maximum response time of the MLD general query packet, in seconds. The valid range is 1-65535.

Defaults

10s.

Command Mode

Global configuration mode.

Usage Guide

Upon receiving the MLD general query packets, the Layer-2 multicast device updates the aging timer of all member ports. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list.

Upon receiving the MLD specific group query packets, the Layer-2 multicast device enables the aging timer of all member ports in this specific group. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface

from the MLD Snooping forwarding list.
For the source query packets of the MLD specific group, the timer is not updated.

Configuration Examples

The following example shows how to set the maximum response time of the MLD general query packet as 100s:

```
Ruijie(config)# ipv6 mld snooping query-max-response-time 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 mld snooping suppression enable

Use this command to enable the MLD Snooping suppression in the global configuration mode. Use the **no** form of this command to disable this function.
ipv6 mld snooping suppression enable
no ipv6 mld snooping suppression enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled.

Command Mode

Global configuration mode.

Usage Guide

With the IPv6 MLD Snooping suppression function enabled, within the query interval, the layer-2 device will only forward the first received MLD Report packet in an IPv6 multicast group to the layer-3 device, but not the other MLD Report packets in the same IPv6 multicast group, reducing the packet number in the network.
This command is used to enable the IPv6 MLD Snooping suppression, and only the MLDv1 Report packets are suppressed rather than the MLDv2 Report packets.

Configuration Examples

The following example shows how to enable MLD Snooping suppression:

```
Ruijie(config-if)# ipv6 mld snooping suppression
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

ipv6 mld snooping vlan

Use this command to enable the MLD Snooping function for the specified vlan. Use the no form of this command to disable this function.

ipv6 mld snooping vlan *vid*

no ipv6 mld snooping vlan *vid*

Parameter Description

Parameter	Description
vid	The vlan id number. The valid range is 1-4094

Defaults By default, the MLD Snooping is enabled in all VLANs.

Command Mode Global configuration mode.

Usage Guide By default, the MLD Snooping is enabled in all VLANs. You can disable the MLD Snooping for the specified vlan.

Configuration Examples The following example shows how to disable the MLD Snooping function in vlan1:

```
Ruijie(config)# no ipv6 mld snooping vlan 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

ipv6 mld snooping vlan mrouter interface

Use this command to set the static mrouter interface. Use the no form of this command to delete a static mrouter interface.

ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

no ipv6 mld snooping vlan *vid* **mrouter interface** *interface-type interface-number*

Parameter Description

Parameter	Description
vid	The vlan id, with the valid range 1-4094.
interface-type interface-number	The interface name.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

Use this command to set the static mrouter interface for the purpose that all IPv6 multicast data received on the switch can be forwarded. With the source port check function enabled, only the multicast flow through the mroute interface can be forwarded.

Configuration Examples

The following example shows how to set a multicast routing port:

```
Ruijie(config)# ipv6 mld snooping vlan 1 mrouter interface fastEthernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

ipv6 mld snooping vlan mrouter learn

Use this command to enable the switch to dynamically learn MLD query or PIM packets to identify the mrouter interface automatically. Use the no form of this command to restore it to cancel the dynamic learning.

ipv6 mld snooping vlan *vid* **mrouter learn**
no ipv6 mld snooping vlan *vid* **mrouter learn**

Parameter Description

Parameter	Description
vid	The vlan id, with the valid range 1-4094.

Defaults

Disabled.

Command Mode

Global configuration mode.

Usage Guide

The mrouter interface is the interface of the multicast device connected with the peer device. By default, the dynamically-learned mroute interface is enabled on the layer-2 multicast device. Use the **no** option to disable this function and clear all dynamically-learned mroute interfaces. With the source port check enabled, only the multicast flow through the mroute interface are valid and forwarded to the registered interface on the layer-2 multicast device. Those multicast flow through the non-mroute interface are invalid and will be discarded. With the source port check function enabled, use the dynamically-learned mroute interfaces to improve the MLD Snooping flexibility.

Configuration Examples

The following example shows how to enable the dynamic multicast route port learn function:

```
Ruijie(config)# ipv6 mld snooping vlan 1 mrouter learn
```

Related Commands

Command	Description
ipv6 mld snooping vlan mrouter interface	Set the mrouter interface.

Platform Description

N/A

ipv6 mld snooping vlan static interface

Use this command to set a static member port to receive the multicast flow for the purpose of preventing the port from being influenced by the MLD Report packets with the MLD Snooping enabled. Use the no form of this command to delete a static member port

ipv6 mld snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

no ipv6 mld snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*

Parameter Description

Parameter	Description
vid	The vlan id, with the valid range 1-4094.
group-address	The multicast address.
interface-type *interface-number*	The interface name.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

Use this command to set the interface as the member port of multiple static multicast addresses.

Configuration Examples

The following example shows how to set the interface fastEthernet 0/1 as the static member port of the FF88::1 group:

```
Ruijie(config)# ipv6 mld snooping vlan 1 static FF88::1 interface fastEthernet
0/1
```

Related Commands

Command	Description
ipv6 mld snooping vlan mrouter interface	Set the mrouter interface.

Platform Description

N/A

permit

Use this command to allow the multicast flow profile within the specified range in the profile configuration mode.

permit

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default profile action is deny.

Command Mode

Profile configuration mode.

Usage Guide

Before configuring this command, use the **range** command to set the multicast range first.

Configuration Examples

The following example shows how to allow the multicast flow profile within the range of FF77::1 to be forwarded only:

```
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)# range FF77::1
Ruijie(config-profile)# permit
```

Related Commands

Command	Description
ipv6 mld profile	Create one profile.
range	Set the multicast address range.
deny	Set the profile action deny.

Platform Description

N/A

range

Use this command to specify the profile multicast flow range, which can be one single multicast address, or can be the multicast address within the specified range when configuring a profile in the profile configuration mode. Use the **no** form of this command to remove the specified multicast address.

range *low-ipv6-address* [*high-ipv6-address*]
no range *low-ipv6-address* [*high-ipv6-address*]

Parameter Description

Parameter	Description
low-ipv6-address	The low address within the specified range.

high-ipv6-address	The high address within the specified range.

Defaults

N/A

Command Mode

Profile configuration mode.

Usage Guide

The value of low-ipv6-address shall be smaller than the one of high-ipv6-address. With the address range configured, an action shall be specified, and the default profile action is deny.

Configuration Examples

The following example shows how to create the multicast flow profile within the range of FF77::1~FF77::100:

```
Ruijie(config)# ipv6 mld profile 1
Ruijie(config-profile)# range FF77::1 FF77::100
```

Related Commands

Command	Description
ipv6 mld profile	Create one profile.
deny	Set the profile action deny.
permit	Set the profile action permit.

Platform Description

N/A

show ipv6 mld profile

Use this command to show the related MLD profile configurations.

show ipv6 mld profile [*profile-number*]

Parameter Description

Parameter	Description
-	Show the configurations of all profiles.
profile-number	Show the configuration of the specified profile.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to show the related MLD profile configurations.

Configuration Examples

The following example shows the MLD profile configurations:

```
Ruijie# show ipv6 mld profile 1
MLD Profile 1
permit
```

```
range FF77::1 FF77::100
range FF88::123
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show ipv6 mld snooping

Use this command to show the related MLD Snooping information.

show ipv6 mld snooping [**gda-table** | **interfaces** | **mrouter** | **statistics** | **vlan** *vlan-id*]

Parameter Description

Parameter	Description
-	Show the MLD Snooping configurations.
gda-table	Show the multicast forwarding rule table.
interfaces	Show the MLD Snooping filtering configuration.
mrouter	Show the information about mrouter interface.
statistics	Show the snooping statistics.
vlan *vlan-id*	Show the snooping information of the specified vlan.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to show the related MLD Snooping information.

Configuration Examples

The following example shows the MLD Snooping configurations using the **show ipv6 mld snooping** command:

```
Ruijie# show ipv6 mld snooping
MLD-snooping mode      : IVGL
SVGL vlan-id           : 1
SVGL profile number     : 0
Source check port      : Disabled
Query max respone time : 10(Seconds)
```

The following example shows the mrouter interface of the MLD Snooping using the **show ipv6 mld snooping statistics** command:

```
Ruijie# show ipv6 mld snooping statistics
GROUP   Interface  Last report    Last leave     Last
                        time        time         reporter
```

```
-------------------------- ------------- -------------
FF88::1 VL1:Gi4/2   0d:0h:0m:7s     ----    2003::1111
                      Report pkts: 1       Leave pkts: 0
```

The following example shows the mrouter interface of the MLD Snooping using the **show ipv6 mld snooping mrouter** command:

```
Ruijie# show ipv6 mld snooping mrouter
Vlan   Interface       State     MLD profile number
----     --------         -------     -------------------
1   GigabitEthernet 0/7    static        1
1   GigabitEthernet 0/12   dynamic       0
```

The following example shows the multicast group information in the GDA table and all member ports information of one multicast group:

```
Ruijie# show ipv6 mld snooping gda-table
Abbr: M - mrouter
     D - dynamic
     S - static
VLAN  Address            Member ports
---------------------------------------------------------
1      FF88::1         GigabitEthernet 0/7(S)

```

The following example shows the MLD Snooping filtering configuration using the **show ipv6 mld snooping mrouter** command:

```
Ruijie# show ipv6 mld snooping interface GigabitEthernet 0/7
Interface        Filter Profile number     max-groups
----------       ----------------------    -----------
GigabitEthernet 0/7          1              4294967294
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

Multicast Forwarding Control Configuration Commands

debug msf api

Use this command to turn on the debugging switch to show the calling operation of the API interface provided by the IPv4 multi-layer multicast forwarding. The **no** form of this command turns off the debugging switch.

debug msf api

no debug msf api

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf6 api

Use this command to turn on the debugging switch to show the calling operation of the API interface provided by the IPv6 multi-layer multicast forwarding. The **no** form of this command turns off the debugging switch.

debug msf6 api

no debug msf6 api

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf event

Use this command to turn on the debugging switch to show the operation of the IPv4 multi-layer multicast forwarding event. The **no** form of this command turns off the debugging switch.

debug msf event

no debug msf event

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf6 event

Use this command to turn on the debugging switch to show the operation of the IPv6 multi-layer multicast forwarding event. The **no** form of this command turns off the debugging switch.

debug msf6 event

no debug msf6 event

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf forwarding

Use this command to turn on the debugging switch to show the operation of IPv4 multi-layer multicast forwarding. The **no** form of this command turns off the debugging switch.

debug msf forwarding

no debug msf forwarding

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf6 forwarding

Use this command to turn on the debugging switch to show the operation of IPv6 multi-layer multicast forwarding. The **no** form of this command turns off the debugging switch.

debug msf6 forwarding

no debug msf6 forwarding

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf msc

Use this command to turn on the debugging switch to show the operation of IPv4 multi-layer multicast forwarding entries. The **no** form of this command turns off the debugging switch.

debug msf msc

no debug msf msc

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf6 msc

Use this command to turn on the debugging switch to show the operation of IPv6 multi-layer multicast forwarding entries. The **no** form of this command turns off the debugging switch.

debug msf6 msc

no debug msf6 msc

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf ssp

Use this command to turn on the debugging switch to show the operation of IPv4 multi-layer multicast forwarding hardware. The **no** form of this command turns off the debugging switch.

debug msf ssp

no debug msf ssp

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

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 msf6 ssp

Use this command to turn on the debugging switch to show the operation of IPv6 multi-layer multicast forwarding hardware. The **no** form of this command turns off the debugging switch.

debug msf6 ssp

no debug msf6 ssp

Parameter

Parameter	Description

Description

N/A	N/A

Defaults

Disabled

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

msf nsf

Use this command to configure the parameters for multicast non-stop forwarding.

msf nsf { **convergence-time** *time* | **leak** *interval* }

no msf nsf {**convergence-time** | **leak**}

Parameter Description

Parameter	Description
convergence-time *time*	Maximum time for the multicast protocol convergence, in the valid range of the 0-3600s. The default value is 70 seconds.
leak *interval*	Packet multicast leak time, in the valid range of 0-3600s. The default value is 80 seconds.

Defaults

Convergence time: 70 seconds;

Leak interval: 80 seconds

Command mode

Global configuration mode

Usage Guide

This command can be configured on the switches supporting hot-standby.

Configuration Examples

```
Ruijie (config)# msf nsf convergence-time 300 leak 20
```

Related

Command	Description

Commands

N/A	N/A

Platform Description

N/A

show msf msc

Use this command to show IPv4 multi-layer multicast forwarding table.

show msf msc [*source-address*] [*group-address*] [*vlan-id*]

Parameter Description

Parameter	Description
source-address	Specified source IP address of the multi-layer multicast forwarding table.
group-address	Specified group address of the multi-layer multicast forwarding table.
vlan-id	The Vlan id where the incoming interface of the multi-layer multicast forwarding table is. The value greater than 4096 indicates a routed port.

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

The three parameters in this command are optional.

If only the source address is specified as s1, all msc entries with source address 1 are displayed.

- If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed.
- If the source address is specified as s1, the group address as g1 and the vlan id as v1, all corresponding msc entries are displayed.

Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.

Configuration Examples

The following example shows the IPv4 layer-3 multicast forwarding entries with source IP address 192.168.195.25:

```
Ruijie# show msf msc 192.168.195.25
Multicast Switching Cache Table
(192.168.195.23, 233.3.3.3, 1), SYNC, MTU:0, 1 OIFs
VLAN 1(0): 1 OPORTs, REQ: DONE
OPORT 6, IGMP-SNP, REQ: DONE
```

The fields in the execution of the **show msf msc** command are described in the following table.

Field	Description
192.168.195.23	Source address of the entry.
233.3.3.3	Group address of the entry.
1	Vlan id where the incoming interface of the entry is.
SYNC	The entry has been synchronized to the hardware.
MTU	MTU value
OIFs	Layer-3 outgoing interface number.
VLAN1(0)	The vlan where the layer-3 outgoing interface oif is.
1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.
REQ: DONE	This oif configuration on the hardware has done.
OPORT 6	The layer-2 port in the oif with index 6.
IGMP-SNP	This port is created by the IGMP SNOOPING protocol. This value can also be the PIM-SNP, which means this port is created by the PIM SNOOPING protocol. And the ROUTER means this port is created by the layer-3 protocol.
REQ: DONE	The port configuration on the hardware has done.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show msf6 msc

Use this command to show IPv6 multi-layer multicast forwarding table.

show msf6 msc [*source-address*] [*group-address*] [*vlan-id*]

Parameter Description

Parameter	Description
source-address	Specified source IP address of the multi-layer multicast forwarding table.
group-address	Specified group address of the multi-layer multicast forwarding table.
vlan-id	The Vlan id where the incoming interface of the multi-layer multicast forwarding table is. The value greater than 4096 indicates a routed port.

Defaults Disabled

Command mode Privileged EXEC mode

Usage Guide The three parameters in this command are optional.

If only the source address is specified as s1, all msc entries with source address 1 are displayed.

- If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed.
- If the source address is specified as s1, the group address as g1 and the vlan id as v1, all corresponding msc entries are displayed.

Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.

Configuration Examples

N/A

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show msf nsf

Use this command to show the configuration of multicast non-stop forwarding.

show msf nsf

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled

Command mode

Privileged EXEC mode

Usage Guide

This command can be configured on the switches supporting hot-standby.

Configuration Examples

```
Ruijie# show msf nsf
Multicast HA Parameters
-------------------------------------------------------------
protocol convergence timeout             120 secs
flow leak interval                      20 secs
```

Related Commands

Command	Description
msf nsf	Configures the parameters for multicast non-stop forwarding.

Platform Description	N/A

Security Configuration Commands

1. AAA Configuration Commands
2. RADIUS Configuration Commands
3. TACACS+ Configuration Commands
4. 802.1X Configuration Commands
5. SSH Configuration Commands
6. Port-based Flow Control Configuration Commands
7. CPU Protection Configuration Commands
8. DoS Protection Configuration Commands
9. DHCP Snooping Configuration Commands
10. DAI Configuration Commands
11. IP Source Guard Configuration Commands
12. ND Snooping Configuration Commands
13. DHCPv6 Snooping Configuration Commands
14. Anti-arp-spoofing Configuration Commands
15. NFPP Configuration Commands

AAA Configuration Commands

aaa accounting commands

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting commands *level* {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting commands *level* {**default** | *list-name*}

Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><i>level</i></td><td>The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.</td></tr>
<tr><td><b>default</b></td><td>When this parameter is used, the following defined method list is used as the default method for command accouting.</td></tr>
<tr><td><i>list-name</i></td><td>Name of the command accouting method list, which could be any character strings.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>none</b></td><td>Do not perform accouting.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for acouting, the TACACS+ server group is supported.</td></tr>
</table>
</td></tr>
</table>

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.

The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Examples

The following example performs accounting of the network service requests from users 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	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the accouting commands to the terminal line.

aaa accounting exec

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting exec {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting exec {**default** | *list-name*}

Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>default</b></td><td>When this parameter is used, the following defined method list is used as the default method for Exec accouting.</td></tr>
<tr><td><i>list-name</i></td><td>Name of the Exec accouting method list, which could be any character strings.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>none</b></td><td>Do not perform accouting.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for acouting, the RADIUS and TACACS+ server group is supported.</td></tr>
</table></td></tr>
</table>

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS enables the exec accounting function after enabling the login authentication.

After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user loggs in, it does not send the account stop information to the security server when a user loggs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Examples

The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access:

```
Ruijie(config)# aaa accounting network start-stop group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the Exec accouting to the terminal line..

aaa accounting network

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting network {**default** | *list-name*} **start-stop group radius**

no aaa accounting network {**default** | *list-name*}

Parameter description

Parameter	Description
network	Perform accounting of the network related service requests, including dot1x, PPP, etc.
resource	Perform accounting of resource related service requests.
list-name	Name of the accounting method list
start-stop	Send accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.

group	Use the server group for accounting.
radius	Use the RADIUS group for accounting.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS performs accounting of user activities by sending record attributes to the security server. Use the keyword **start-stop** to set the user accounting option.

Examples

The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access:

```
Ruijie(config)# aaa accounting network start-stop group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization network	Define a network authorization method list.
aaa authentication	Define AAA authentication.
username	Define a local user database.

aaa accounting update

Use this command to enable the accounting update function The **no** form of this command is used to disable the accounting update function.

aaa accounting update

no aaa accounting update

Parameter description

N/A.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Examples

The following example demonstrates how to enable the accounting update function.

```
Ruijie(config)# aaa new-model
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accounting network	Define a network accounting method list.

aaa accounting update periodic

If the accounting update function has been enabled, use this command to set the interval of sednign the accounting update message. The **no** form of this command is used to restore it to the default value.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter description

Parameter	Description
interval	Interval of sending the accounting update message, in minute. The shortest interval is 1 minute.

Default

5 minutes.

Command mode

Global configuration mode.

Usage guidelines

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Examples

The following example demonstrates how to set the interval of accounting update to 1 minute.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
Ruijie(config)# aaa accounting update periodic 1
```

Related

Command	Description

commands	**aaa new-model**	Enable the AAA security service.
	aaa accounting network	Define a network accounting method list.

aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list. The **no** form of this command is used to delete the 802.1x user authentication method list.

aaa authentication dot1x {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication dot1x {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.
list-name	Name of the 802.1x user authentication method list, which could be any character string.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS server group is supported.

Default	N/A

Command mode	Global configuration mode.

Usage guidelines

If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use **aaa authentication dot1x** to configure a default or optional method list for 802.1x user authentication.

The next method can be used for authentication only when the current method does not work.

Examples

The following example defines an AAA authentication method list named **RDS_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication dot1x rds_d1x group radius local
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
dot1x authentication	Associate a specific method list with the 802.1x user.
username	Define a local user database.

aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list. The **no** form of this command is used to delete the user authentication method list.

aaa authentication enable {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication enable default

Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>default</b></td><td>When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>local</b></td><td>Use the local user name database for authentication.</td></tr>
<tr><td><b>none</b></td><td>Do not perform authentication.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.</td></tr>
</table></td></tr>
</table>

Default

N/A

Command mode

Global configuration mode.

Usage

If the AAA Enable authentication service is enabled on the device,

guidelines

users must use AAA for Enable authentication negotiation. You must use **aaa authentication enable** to configure a default or optional method list for Enable authentication.

The next method can be used for authentication only when the current method does not work.

The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

Examples

The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication enable default group radius
local
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
enable	Switchover the user level.
username	Define a local user database.

aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list. The **no** form of this command is used to delete the authentication method list.

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

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

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
list-name	Name of the user authentication method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.

Keyword	Description
local	Use the local user name database for authentication.
none	Do not perform authentication.
group	Use the server group for authentication. At present, the RADIUS and TACACS+

	server groups are supported.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use **aaa authentication login** to configure a default or optional method list for Login authentication.

The next method can be used for authentication only when the current method does not work.

You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

Examples

The following example defines an AAA Login authentication method list named **list-1**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication login list-1 group radius local
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
login authentication	Apply the Login authentication method to the terminal lines.
username	Define a local user database.

aaa authentication ppp

Use this command to enable AAA PPP user authentication and configure the PPP user authentication method list. The **no** form of this command is used to delete the authentication method list.

aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication ppp {**default** | *list-name*}

Parameter description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.

<table>
<tr><td><i>list-name</i></td><td>Name of the user authentication method list, which could be any character strings.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>local</b></td><td>Use the local user name database for authentication.</td></tr>
<tr><td><b>none</b></td><td>Do not perform authentication.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for authentication. At present, the RADIUS server group is supported.</td></tr>
</table>
</td></tr>
</table>

Default

N/A

Command mode

Global configuration mode.

Usage guidelines

If the AAA PPP security service is enabled on the device, users must use AAA for PPP authentication negotiation. You must use **aaa authentication ppp** to configure a default or optional method list for PPP user authentication.

The next method can be used for authentication only when the current method does not work.

Examples

The following example defines an AAA PPP authentication method list named **rds_ppp**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Ruijie(config)# aaa authentication ppp rds_ppp group radius local
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
ppp authentication	Associate a specific method list with the PPP user.
username	Define a local user database.

authorization commands

Use this command to apply the list of command authorization to the specific terminal line in the line configuration mode. The **no** form of this command is used to disable this function.

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

no authorization commands *level*

Parameter description

Parameter	Description
level	The authorized command level, 0-15.
default	Use the default command authorization command.
list-name	Apply a defined method list of the command authorization.

Default

Disabled.

Command mode

Line configuration mode.

Usage guidelines

Once the default command authorization method list has been configured, it is applied to all terminals automatically. Once the non-default command authorization method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the command authorization in this line is ineffective tilll the authorization method list is defined.

Examples

The following example configures the command authorization method list with name cmd, authorizes command level 15, uses the TACACS+ server. If the security server does not response, it does not perform authorization. After configuration, the authorization command is applied to VTY 0-4 lines:

```
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	Enable the AAA security service.
aaa authorization	Define the method list of the AAA command authorization.

commands	

login authentication

Use this command to apply the Login authentication method list to the specified terminal lines. The **no** form of this command is used to remove the application of Login authentication method list.

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

no login authentication

Parameter description

Parameter	Description
default	Apply the default Login authentication method list to the terminal line.
list-name	Apply the defined Login authentication method list to the terminal line.

Default

N/A

Command mode

Line configuration mode.

Usage guidelines

Once the default login authentication method list has been configured, it will be applied to all the terminals automatically. If non-default login authentication method list has been applied to the terminal, it will replace the default one. If you attempt to apply the undefined method list, it will prompt a warning message that the login authentication in this line is ineffective till it is defined.

Examples

The following example defines an AAA Login authentication method list named **list-1**. In the authentication method list, first the local user database is used for authentication. 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	Enable the AAA security service.
login authentication	Configure the Login authentication method list.
username	Define a local user database.

aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI. The **no** form of this command is used to disable the aaa authorization command function.

aaa authorization commands *level* {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization commands *level* {**default** | *list-name*}

Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><i>level</i></td><td>Command level to be authorized, 0-15.</td></tr>
<tr><td><b>default</b></td><td>When this parameter is used, the following defined method list is used as the default method for command authorization.</td></tr>
<tr><td><i>list-name</i></td><td>Name of the user authorization method list, which could be any character strings.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>none</b></td><td>Do not perform authorization.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for authorization. At present, the RADIUS server group is supported.</td></tr>
</table></td></tr>
</table>

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny.

It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.

The configured command authorization method must be applied to terminal line which requires for the command authorization. Otherwise, the configured command authorization method is ineffective.

Examples

The following example uses the TACACS+ server to authorize the level 15 command:

```
Ruijie(config)# aaa authorization commands 15 default group tacacs+
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
authorization commands	Apply the command authorization for to the terminal line.

aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode). The **no** form of this command is used to disable the configuration command authorization function.

aaa authorization config-commands

no aaa authorization config-commands

Parameter description

N/A

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.

Examples

The following example enables the configuration command authorization function:

```
Ruijie(config)# aaa authorization config-commands
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the AAA command authorization.

aaa authorization console

Use this command to authorize the commands of the users who has logged in the console. The **no** form of this command is used to disable the authorization function.

aaa authorization console

no aaa authorization console

Parameter description

N/A

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.

Examples

The following example enables the aaa authorization console function:

```
Ruijie(config)# aaa authorization console
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization commands	Define the AAA command authorization.
authorization commands	Apply the command authorization to the terminal line..

aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level. The **no** form of this command is used to disable the aaa authorization exec function.

aaa authorization exec {**default** | *list-name*} *method1* [*method2*...]

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

Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>default</b></td><td>When this parameter is used, the following defined method list is used as the default method for Exec authorization.</td></tr>
<tr><td><i>list-name</i></td><td>Name of the user authorization method list, which could be any character strings.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>local</b></td><td>Use the local user name database for authorization.</td></tr>
<tr><td><b>none</b></td><td>Do not perform authorization.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for authorization. At present, the RADIUS server group is supported.</td></tr>
</table>
</td></tr>
</table>

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level(0-15). The aaa authorization exec function is effective on condition that Login authentication function has been enabled. It can not enter the CLI if it fails to enable the aaa authorization exec.

You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

Examples

The following example uses the RADIUS server to authorize Exec:

```
Ruijie(config)# aaa authorization exec default group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
authorization exec	Apply the command authorization to the terminal line .
username	Define a local user database.

aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network. The **no** form of this command is used to disable the authorization function.

aaa authorization network {**default** | *list-name*} *method1* [*method2*...]

no aaa authorization network {**default** | *list-name*}

Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>default</b></td><td>When this parameter is used, the following defined method list is used as the default method for Network authorization.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>none</b></td><td>Do not perform authorization.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for authorization. At present, the RADIUS server group is supported.</td></tr>
</table>
</td></tr>
</table>

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.

Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.

The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

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	Enable the AAA security service.
aaa accounting	Define AAA accounting .
aaa authentication	Define AAA authentication.
username	Define a local user database.

aaa authorization exec

Use this command to apply the Exec authorization methos list to the specified terminal lines in the line configuration mode. The **no** form of this command is used to disable the authorization function.

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

no authorization exec

Parameter description

Parameter	Description
default	Use the default method of Exec authorization.
list-name	Apply a defined method list of Exec authorization.

Default

Disabled.

Command mode

Line configuration mode.

Usage guidelines

Once the default execauthorization method list has been configured, it is applied to all terminals automatically. Once the non-default command authorization method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the exec authorization in this line is ineffective tilll the authorization method list is defined.

Examples

The following example configures the exec authorization method list with name exec-1, uses the RADIUS server. If the security server does not response, it does not perform authorization. After configuration, the authorization command is applied to VTY 0-4 lines:

```
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	Enable the AAA security service.
aaa authorization commands	Define the method list of AAA Exec authorization.

aaa accounting commands

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the 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	The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.
default	When this parameter is used, the following defined method list is used as the default method for command accouting.
list-name	Name of the command accouting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods. Keyword: Description **none**: Do not perform accouting. **group**: Use the server group for acouting, the TACACS+ server group is supported.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.

The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Examples

The following example performs accounting of the network service requests from users 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	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the accouting commands to the terminal line.

aaa accounting exec

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting exec {**default** | *list-name*} **start-stop** *method1* [*method2*...]

no aaa accounting exec {**default** | *list-name*}

Parameter description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>default</b></td><td>When this parameter is used, the following defined method list is used as the default method for Exec accouting.</td></tr>
<tr><td><i>list-name</i></td><td>Name of the Exec accouting method list, which could be any character strings.</td></tr>
<tr><td><i>method</i></td><td>It must be one of the keywords listed in the following table. One method list can contain up to four methods.
<table>
<tr><th>Keyword</th><th>Description</th></tr>
<tr><td><b>none</b></td><td>Do not perform accouting.</td></tr>
<tr><td><b>group</b></td><td>Use the server group for acouting, the RADIUS and TACACS+ server group is supported.</td></tr>
</table>
</td></tr>
</table>

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS enables the exec accounting function after enabling the login authentication.

After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user loggs in, it does not send the account stop information to the security server when a user loggs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Examples

The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access:

```
Ruijie(config)# aaa accounting network start-stop group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authentication	Define AAA authentication.
accouting commands	Apply the Exec accouting to the terminal line..

aaa accounting network

Use this command to account users in order to count the network access fees or manage user activities. The **no** form of this command is used to disable the accounting function.

aaa accounting network {**default** | *list-name*} **start-stop group radius**

no aaa accounting network {**default** | *list-name*}

Parameter description

Parameter	Description
network	Perform accounting of the network related service requests, including dot1x, PPP, etc.
resource	Perform accounting of resource related service requests.

list-name	Name of the accounting method list
start-stop	Send accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
group	Use the server group for accounting.
radius	Use the RADIUS group for accounting.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

RGOS performs accounting of user activities by sending record attributes to the security server. Use the keyword **start-stop** to set the user accounting option.

Examples

The following example performs accounting of the network service requests from users using RADIUS, and sends the accounting messages at the start and end time of access:

```
Ruijie(config)# aaa accounting network start-stop group radius
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa authorization network	Define a network authorization method list.
aaa authentication	Define AAA authentication.
username	Define a local user database.

aaa accounting update

Use this command to enable the accounting update function The **no** form of this command is used to disable the accounting update function.

aaa accounting update

no aaa accounting update

Parameter description

N/A.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Examples

The following example demonstrates how to enable the accounting update function.

```
Ruijie(config)# aaa new-model
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accounting network	Define a network accounting method list.

aaa accounting update periodic

If the accounting update function has been enabled, use this command to set the interval of sednign the accounting update message. The **no** form of this command is used to restore it to the default value.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter description

Parameter	Description
interval	Interval of sending the accounting update message, in minute. The shortest interval is 1 minute.

Default

5 minutes.

Command mode

Global configuration mode.

Usage guidelines

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Examples

The following example demonstrates how to set the interval of accounting update to 1 minute.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
Ruijie(config)# aaa accounting update periodic 1
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa accounting network	Define a network accounting method list.

accounting commands

Use this command to apply the accounting command list to the specified terminal lines. The **no** form of this command is used to disable the accounting function.

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

no accounting commands *level*

Parameter description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before determing which command level is executed.
default	Use the default method of accouting commands.
list-name	Use a defined command accouting method list.

Default

Disabled.

Command mode

Line configuration mode.

Usage guidelines

Once the default command accouting method list has been configured, it is applied to all terminals automatically. Once the non-default command accounting method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the command authorization in this line is ineffective till the accounting command method list is defined.

Examples

The following example configures the accounting command method list with name cmd, accounts the level-15 command, uses the TACACS+ server. If the security server does not response, it does not perform accounting. After configuration, the accounting command is applied to VTY 0-4 lines:

```
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	Enable the AAA security service.
aaa accouting commands	Define the method list of AAA accouting command.

accounting exec

Use this command to apply the exec accouting method list to the specified terminal lines in the line configuration mode. The **no** form of this command is used to disable the exec accounting function.

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

no accounting exec

Parameter description

Parameter	Description
default	Use the default method of Exec accouting.
list-name	Use a defined Exec accouting method list.

Default

Disabled.

Command mode

Line configuration mode.

Usage guidelines

Once the default exec accouting method list has been configured, it is applied to all terminals automatically. Once the non-default exec accounting method list has been configured, it is applied to the line instead of the default method list. If you attempt to apply a undefined method list, a warning message will prompt that the exec accounting in this line is ineffective till the exec accounting command method list is defined.

Examples

The following example configures the exec accounting method list with name exec-1, uses the RADIUS server. If the security server does not response, it does not perform accounting. After configuration, the exec accounting is applied to VTY 0-4 lines:

```
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	Enable the AAA security service.
aaa accouting commands	Define the method list of AAA Exec accouting.

aaa domain

Use this command to configure the domain attributes.The **no** form of this command is used to remove the setting.

aaa domain {**default** | *domain-name*}

no aaa domain {**default |** *domain-name*}

Parameter description

Parameter	Description
default	Use this parameter to configure the default domain.
domain-name	The name of the specified domain.

Default No domain is configured.

Command mode Global configuration mode.

Usage guidelines Use this command to configure the domain-name–based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this domain name, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

Examples The following example configures the domain name.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)#
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.

aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

aaa domain enable

Use this command to enable domain-name-based AAA service, which is disabled by default. The **no** form of this command is used to disable the service.

aaa domain enable

no aaa domain enable

Parameter description

N/A.

Default

disabled

Command mode

Global configuration mode.

Usage guidelines

To perform the domain-name-based AAA service configuration, enable this service.

Examples

The following example enables the domain-name-based AAA service.

```
Ruijie(config)# aaa domain enable
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
show aaa doamin	Show the domain configuration.

access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users. The **no** form of this command is used to remove the setting.

access-limit *num*

no access-limit

Parameter description

Parameter	Description
num	The number used for the user limitation is only valid for the IEEE802.1 users.

Default

By default, no number of users is limited.

Command mode

Domain configuration mode.

Usage guidelines

This command limits the number of users for the domain.

Examples

The following example sets the number of users as 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	Enable the AAA security service.
enable	Switchover the user level.
username	Define a local user database.

accounting network

Use this command to configure the Network accounting list. The **no** form of this command is used to remove the setting.

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

no accounting network

Parameter description

Parameter	Description
default	Use this parameter to specify the default method list.
list-name	The name of the network accounting list.

Default

With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.

Command mode

Domain configuration mode.

Usage guidelines

Use this command to configure the Network accounting method list for the specified domain.

Examples

The following example sets the Network accounting method list for the specified domain.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# accounting network default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

authentication dot1x

Use this command to configure the IEEE802.1x authentication list. The **no** form of this command is used to remove the setting.

authentication dot1x {**default** | *list-name*}

no authentication dot1x

Parameter description

Parameter	Description
default	Use this parameter to specify the default method list
list-name	The name of the specified method list

Default

With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command mode

Domain configuration mode.

Usage guidelines

Specify an IEEE802.1x authentication method list for the domain.

Examples

The following example sets an IEEE802.1x authentication method list for the specified domain.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# authentication dot1x default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

authorization network

Use this command to configure the Network authorization list. The **no** form of this command is used to remove the setting.

authorization network {**default** | *list-name*}

no authorization network

Parameter description

Parameter	Description
default	Use this parameter to specify the default method list
list-name	The name of the specified method list.

Default

With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command mode

Domain configuration mode.

Usage guidelines

Specify an authorization method list for the domain.

Examples

The following example sets an authorization method list for the specified domain.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# authorization network default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain	Enable the domain-name-based

enable	AAA service.
show aaa domain	Show the domain configuration.

show aaa domain

Use this command to show all current domain information

show aaa domain [**default** | *domain-name*]

Parameter description

Parameter	Description
default	Use this parameter to show the default domain.
domain-name	Show the specified domain.

Default

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

If no domain-name is specified, all domain information will be displayed.

Examples

The following example shows the domain named domain.com

```
Ruijie(config)# show aaa domain domain.com
=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.

state

Use this command to set whether the configured domain is valid. The **no** form of this command restore it to the default setting.

state {**block | active**}

no state

Parameter description

Parameter	Description
block	The configured domain is invalid.
active	The configured domain is valid.

Default

Active

Command mode

Domain configuration mode.

Usage guidelines

Use this command to set whether the specified configured domain is valid.

Examples

The following example set 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	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain enable	Show the domain configuration .

username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers. The **no** form of this command restores it to the default setting.

username-format {**without-domain**| **with-domain**}

no username-format

Parameter description

Parameter	Description
without-domain	Set the user name without the domain

	information.
with-domain	Set the user name with the domain information.

Default Without-domain

Command mode Domain configuration mode.

Usage guidelines Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Examples The following example sets the user name without the domain information.

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# username-domain without-domain
```

Related commands

Command	Description
aaa new-model	Enable the AAA security service.
aaa domain enable	Enable the domain-name-based AAA service.
show aaa domain	Show the domain configuration.

aaa group server

Use this command to configure the AAA server group. The **no** form of this command is used to delete the server group.

aaa group server {**radius** | **tacacs+**} *name*

no aaa group server {**radius** | **tacacs+**} *name*

Parameter description

Parameter	Description
name	Name of the server group. It cannot be the keywords "**radius"** and "**tacacs+**".

Command mode Global configuration mode.

Usage This command is used to configure the AAA server group. Currently,

guidelines

the RADIUS and TACACS+ server groups are supported.

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	Show the AAA server group information.

ip vrf forwarding

Use this command to select the **vrf** for the AAA server group. The **no** form of this command removes the setting.

ip vrf forwarding *vrf_name*

no ip vrf forwarding

Parameter description

Parameter	Description
vrf_name	VRF name

Default Configuration

N/A.

Command mode

Server group configuration mode.

Usage guidelines

This command selects VRF for the specified server groups.

Examples

The following example selects the VRF for the 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	Configure the AAA server group.
show aaa group	Show the AAA server group information.

server

Use this command to add a server to the AAA server group. The **no** form is used to delete a server.

server *ip-addr* [**authen-port** *port1*] [**acct-port** *port2*]

no server *ip-addr* [**authen-port** *port1*] [**acct-port** *port2*]

Parameter description

Parameter	Description
ip-addr	IP address of the server
port1	Authentication port of the server
port2	Accounting port of the server

Default

No server is configured.

Command mode

Server group configuration mode.

Usage guidelines

Add a server to the specified server group. The default value is used if no port is specified.

Examples

The following example adds a server to the server group.

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.12
acct-port 5 authen-port 6
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Group-name:  ss
Group Type:  radius
Referred:   2
Server List:
IP Address: 192.168.4.12
Authentication Port: 6
Accounting Port: 5
Referred:  1
```

Related commands

Command	Description
aaa group	Configure the AAA server group.

server	
show aaa group	Show the AAA server group information.

show aaa group

Use this command to show all the server groups configured for AAA.

show aaa group

Parameter description

N/A.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows all the server groups configured for AAA.

```
Ruijie# show aaa group
Group Name:  ss
Group Type:  radius
Referred:   2
Server List:
IP Address: 192.168.217.64
Authentication Port: 1812
Accounting Port: 1813
Referred:  1
```

Related commands

Command	Description
aaa group server	Configure the AAA server group.

aaa local authentication attempts

Use this command to configure login attempt times .

aaa local authentication attempts *max-attempts*

Parameter description	In the range of 1 to 2147483647.
Default	The default value is 3.
Command mode	Global configuration mode.
Usage guidelines	Use this command to configure login attempt times.

Examples

```
Ruijie #configure terminal
Ruijie (config)#aaa local authentication attempts 6
```

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

aaa local authentication lockout-time

Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times .

aaa local authentication lockout-time *lockout-time*

Parameter description	In the range of 1 to 2147483647.
Default	15 hours.
Command mode	Global configuration mode.
Usage guidelines	Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times .

Examples

```
Ruijie#configure terminal
Ruijie(config)#aaa local authentication lockout-time 5
```

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

aaa new-model

Use this command to enable the RGOS AAA security service. The **no** form of this command is used to disable the AAA security service.

aaa new-model

no aaa new-model

Parameter description N/A.

Default Disabled.

Command mode Global configuration mode.

Usage guidelines Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

Examples The following example shows how to enable the AAA security service.

```
Ruijie(config)# aaa new-model
```

Related commands

Command	Description
aaa authentication	Define a user authentication method list.
aaa authorization	Define a user authorization method list.
aaa accouting	Define a user accouting method list.

clear aaa local user lockout

Use this command to clear the lockout user list.

clear aaa local user lockout {all | user-name <*word*>**}**

Parameter description

Parameter	Description
word	User ID.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines Use this command to clear all the user lists or the specified user list.

Examples

```
Ruijie(config)# clear aaa local user lockout all
```

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

debug aaa

Use this command to turn on the AAA service debugging switch. The **no** form of this command is used to turn off the debugging switch.

debug aaa event

no debug aaa event

Parameter description N/A.

Command mode Privileged EXEC mode.

show aaa method-list

Use this command to show all AAA method lists.

show aaa method-list

Parameter description N/A.

Default N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command to show all AAA method lists.

Examples

The following example shows the AAA method list.

```
Ruijie# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local  group angel group rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorizating network default group radius
```

Related commands

Command	Description
aaa authentication	Define a user authentication method list
aaa authorization	Define a user authorization method list
aaa accounting	Define a user accounting method list

show aaa user lockout

Use this command to show the lockout user list.

show aaa local user lockout {all | user-name <*word*>**}**

Parameter description

Parameter	Description
word	User ID.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage

Use this command to show the lockout user list and show how long

guidelines

the lockout-time is.

Examples

```
Ruijie# show aaa user lockout all
```

Related commands

Command	Description
show running-config	Show the current configuration of the switch.
show aaa lockout	Show the lockout configuration parameter of current login.

RADIUS Configuration Commands

ip radius source-interface

Use this command to specify the source IP address for the RADIUS packets. Use the **no** form of this command to delete the source IP address for the RADIUS packet.

ip radius source-interface *interface*

no radius source-interface

Parameter description

Parameter	Description
Interface	Interface that the source IP address of the RADIUS packet belongs to.

Default

The source IP address of the RADIUS packet is set by the network layer.

Command mode

Global configuration mode.

Usage guidelines

In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

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	Define the RADIUS server.
ip address	Configure the IP address of the interface.

radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute in the global configuration mode. Use the **no** form of this command to restore to the default value.

radius-server attribute 31 mac format {**ietf** | **normal** | **unformatted**}

no radius-server attribute 31 mac format

Parameter description

Parameter	Description
ietf	The standard format specified by the IETF RFC3580 . -is used as the seperator, for example: 00-D0-F8-33-22-AC.
normal	Normal format representing the MAC address. .is used as the seperator. For example: 00d0.f833.22ac.
unformatted	No format and seperator. By default, unformatted is used. For example: 00d0f83322ac.

Default

The default format is **unformatted**.

Command mode

Global configuration mode.

Usage guidelines

Some RADIUS security servers(mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

Examples

The following example shows how to define the RADIUS Calling-Station-ID attribute as IETF format:

```
Ruijie(config)# radius-server attribute 31 mac format ietf
```

Related commands

Command	Description
radius-server host	Define the RADIUS server.

radius-server host

Use this command to specify a RADIUS security server host. The **no** form of this command is used 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
hostname	DNS name of the RADIUS security server host.
ip-address	IP address of the RADIUS security server host.
auth-port	UDP port used for RADIUS authentication.
*port-numbe*r	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
acct-port	UDP port used for RADIUS accounting.
port-number	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
test username *name*	(Optional) Enable the active detection to the RADIUS security server and specify the username used by the active detection.
idle-time *time*	(Optional) Set the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
ignore-auth-port	(Optional) Disable the detection to the authentication port on the RADIUS security server. It is enabled by default.
ignore-acct-port	(Optional) Disable the detection to the authentication port on the RADIUS security server. It is enabled by default.

Default

No RADIUS host is specified.

Command mode

Global configuration mode.

Usage

In order to implement the AAA security service using RADIUS, you

guidelines

must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

Examples

The following example defines a RADIUS security server host:

```
Ruijie(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
Ruijie(config)# radius-server host 192.168.100.1 test username
viven idle-time 60 ignore-acct-port
```

The following example defines a RADIUS security server host in the IPv6 environment

```
Ruijie(config)# radius-server host 3000::100
```

Related commands

Command	Description
aaa authentication	Define the AAA authentication method list
radius-server key	Define a shared password for the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server timeout	Define the timeout for the RADIUS packet.

radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server. The **no** form of this command is used 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: Simply-encrypted.

Default

No shared password is specified.

Command mode

Global configuration mode.

Usage guidelines

A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

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	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server timeout	Define the timeout for the RADIUS packet.

radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond. The **no** form of this command is used to restore it to the default setting.

radius-server retransmit *retries*

no radius-server retransmit

Parameter description

Parameter	Description
retries	Number of retransmissions

Default

The default number of retransmissions is 3.

Command mode

Global configuration mode.

Usage guidelines

AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

Examples

The following example sets the number of retransmissions to 4:

```
Ruijie(config)# radius-server retransmit 4
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the timeout for the RADIUS packet.

radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet. The **no** format of this command is used to restore it to the default setting.

radius-server timeout *seconds*

no radius-server timeout

Parameter description

Parameter	Description
seconds	Timeout in the range 1 to1000 seconds.

Default

5 seconds.

Command mode

Global configuration mode.

Usage guidelines

Use this command to change the timeout of packet retransmission.

Examples

The following example sets the timeout to 10 seconds:

```
Ruijie(config)# radius-server timeout 10
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server	Define the number of the RADIUS

retransmit	packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.

radius-server dead-ctriteria

This global configuration command is used to configure criteria on a device to determine that the Radius server is unreachable. The **no** form of this command is used 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*	Configure the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range of 1s to 120s.
tries *number*	Configure the successive timeout times. When sending a request from the device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range of 1 to 100.

Default

time *seconds*: 60s.

tries *number*: 10.

Command mode

Global configuration mode.

Usage guidelines

If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

Examples

The following example sets the timeout to 120s and timeout times to 20.

```
Ruijie(config)# radius-server dead-criteria time 120 tries 20
```

Related

Command	Description

commands

radius-server host	Define the RADIUS security server.
radius-server deadtime	Define the duration when a device stops sending any requests to an unreachable Radius server.
radius-server timeout	Define the timeout for the packet retransmission.

radius-server deadtime

The global configuration command is used to configure the duration when a device stops sending any requests to an unreachable Radius server. The **no** form of this command is used to recover the default value.

radius-server deadtime *minnutes*

no radius-server deadtime

Parameter description

Parameter	Description
minutes	Define the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range of 1 min to 1440 min (24h).

Default

The default value of minutes is 0 min, that is, the device keeps sending requests to the unreachable Radius server.

Command mode

Global configuration mode.

Usage guidelines

If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorted than the unreachable time..

Examples

The following example sets the duration when the device stops sending requests to 1 min.

```
Ruijie(config)# radius-server deadtime 1
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server	Define the criteria to determine that a

dead-criteria	Radius server is unreachable.

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 1 to 255
type	Private attribute type

Default

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	dailup-avoid	21
22	ip privilege	22
23	login privilege	42

Extended attributes:

id	Function	Type
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan-id.	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Command mode

Global configuration mode.

Usage guidelines

Use this command to configure the type value of a private attribute.

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	Set the qos value sent by the RADIUS server as the cos value of the interface.

radius set qos cos

Use this command to set the qos value sent by the RADIUS server as the cos value of the interface. Use the **no** form of this command to restore it to the default setting.

radius set qos cos

no radius set qos cos

Parameter description N/A.

Default Set the qos value sent by the RADIUS server as the dscp value.

Command mode Global configuration mode.

Usage guidelines Set the qos value sent by the RADIUS server as the cos value, and the dscp value by default.

Examples The following example sets the qos value sent by the RADIUS server as the cos value of the interface.:

```
Ruijie(config)# radius set qos cos
```

Related commands

Command	Description
radius vendor-specific extend	Extend RADIUS not to differentiate the IDs of private vendors.

radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors. Use the **no** form of this command to disable the function.

radius vendor-specific extend

no radius vendor-specific extend

Parameter description N/A.

Default Only the private vendor IDs of Ruijie are recognized.

Command mode	Global configuration mode.

Usage guidelines	Use this command to identify the attributes of all vendor IDs by type.

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	Configure vendor type.
radius set qos cos	Set the qos value sent by the RADIUS server as the cos value of the interface.

debug radius

Use this command to turn on the RADIUS debugging switch. The **no** form of this command is used to turn off the RADIUS debugging switch.

debug radius {**event | detail**}

no debug radius {**event | detail**}

Parameter Description	N/A.

Command mode	Privileged EXEC configuration mode.

show radius server

Use this command to show the configuration of the RADIUS server.

show radius server

Parameter description	N/A.
Default	N/A.
Command mode	Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show radius server
erver IP:   192.168.4.12
Accounting  Port:  23
Authen  Port:    77
Test Username:   viven
Test Idle Time:   10 Minutes
Test Ports:       Authen
Server State:    Active
   Current duration 765s, previous duration 0s
   Dead: total time 0s, count 0
   Statistics:
      Authen: request 15, timeouts 1
      Author: request 0, timeouts 0
      Account: request 0, timeouts 0

Server IP:   192.168.4.13
Accounting Port:  45
Authen  Port:    74
Test Username:   <Not Configured>
Test Idle Time:   60 Minutes
Test Ports:       Authen and Accounting
Server State:    Active
   Current duration 765s, previous duration 0s
   Dead: total time 0s, count 0
   Statistics:
      Authen: request 0, timeouts 0
      Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the packet transmission timeout.

show radius parameter

Use this command to show the global parameters of the RADIUS server.

show radius parameter

Parameter description N/A.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples

```
Ruijie# show radius parameter
Server Timout:     5 Seconds
Server Deadtime:   0 Minute
Server Retries:    3
Server Dead Critera:
    Time:       10 Seconds
    Tries:      10
```

Related commands

Command	Description
radius-server host	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the packet transmission timeout.

show radius vendor-specific

Use this command to show the configuration of the private vendors.

show radius vendor-specific

Parameter description N/A.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie#show radius vendor-specific
id   vendor-specific     type-value
----- -------------------- ----------
1    max-down-rate       1
2    port-priority       2
3    user-ip            3
4    vlan-id            4
5    last-supplicant-vers 5
     ion
6    net-ip             6
7    user-name          7
8    password           8
9    file-directory      9
10   file-count         10
11   file-name-0         11
12   file-name-1         12
13   file-name-2         13
14   file-name-3         14
15   file-name-4         15
16   max-up-rate         16
17   current-supplicant-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	Define the RADIUS security server.
radius-server retransmit	Define the number of RADIUS packet retransmissions.
radius-server key	Define a shared password for the RADIUS server.
radius-server timeout	Define the packet transmission timeout.

TACACS+ Configuration Commands

aaa group server tacacs+

Use this command to configure TACACS+ group server, dividing different TACACS+ servers to the different groups.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Parameter description

Parameter	Description
group_name	TACACS+ server group name

Default Configuration

No TACACS+ server group is configured.

Command mode

Global configuration mode.

Usage guidelines

By dividing TACACS+ servers into several groups, the tasks of anthentication, authorization and accounting can be implemented by different server groups.

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
Ruijie(config-gs-tacacs+)# ip vrf forwarding vpn1
```

Related commands

Command	Description
server	Configure server list of TACACS+ server group.
ip vrf forwarding	Configure VRF name supported by TACACS+ server group.

server(TACACS+)

Use this command to configure server address in TACACS+ group server.

server *ip-address*

no server *ip-address*

Parameter description

Parameter	Description
ip-address	server address in TACACS+ group server

Default Configuration

N/A

Command mode

TACACS+ group server configuration mode.

Usage guidelines

You must enter TACACS+ server group configuration mode to configure this command.

To configure server address in TACACS+ group server, you must execute **tacacs-server host** in the global configuration mode.

For the server address in TACACS+ group servers, when one server does not reply, it will send the request to the next server.

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+	Configure TACACS+ server group.
ip vrf forwarding	Configure VRF name supported by TACACS+ server group.

ip vrf forwarding(TACACS+)

Use this command to configure vrf name used by TACACS+ group server (this command exists in the device supporting VRF)

ip vrf forwarding *vrf-name*

no ip vrf forwarding

Parameter description

Parameter	Description
vrf-name	VRF name.

Default Configuration

N/A

Command mode

TACACS+ group server configuration mode.

Usage guidelines

Specify vrf name to the specified TACACS+ server.

Examples

The following example specifies VRF name as vpn1 to TACACS+ server group:

```
Ruijie(config)# aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
Ruijie(config-gs-tacacs+)# ip vrf forwarding vpn1
```

Related commands

Command	Description
aaa group server tacacs+	Configure TACACS+ server group.
server	Configure server list of TACACS+ server group.

ip tacacs source-interface

Use this command to configure the source address of TACACS+ packet:

ip tacacs source-interface *interface*

no ip tacacs source-interface

Parameter description

Parameter	Description
interface	Source address interface of TACACS+ packet

Default Configuration

The source address of TACACS+ packet is set on network layer.

Command mode

Global configuration mode.

Usage

To decrease the work of maintaining massive NAS messages in

guidelines

TACACS+ server, use this command to set the source address of TACACS+ packet. This command specifies the first ip address of the specified interface as the source address of TACACS+ packet and is used on L3 devices.

Examples

The following example specifies TACACS+ packet to obtain ip address from fastEthernet 0/0 as the source address of TACACS+ packet :

```
Ruijie(config)# ip tacacs source-interface fastEthernet 0/0
```

Related commands

Command	Description
tacacs-server host	Define TACACS+ server.
ip address	Configure ip address of the interface.

tacacs-server host

Use this command to configure IP address of 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 TACACS+ server host.
ipv6-address	IPv6 address of TACACS+ server host.
port *integer*	TCP port used in TACACS+ communication.
timeout *integer*	Timeout time of TACACS+ host.
key *string*	Shared keyword of TACACS+ client and server.

Default Configuration

No specified TACACS+ host.

Command mode

Global configuration mode.

Usage guidelines

To use TACACS+ to implement AAA security service, you must define TACACS+ secure server. You can define one or multiple TACACS+ secure servers by using **tacacs-server host.**

Examples

The following example defines a TACACS+ secure server host:

```
Ruijie(config)# tacacs-server host 192.168.12.1

Ruijie(config)# tacacs-server host 2001::1
```

Related commands

Command	Description
aaa authentication	Define AAA identity authentication method list.
tacacs-server key	Define the shared password of TACACS+ secure server globally.
tacacs-server timeout	Define timeout timer of reply packet of TACACS+ server globally.

tacacs-server key

Use this command to configure global password of TACACS+ :

tacacs-server key [*0* | *7*] *string*

no tacacs-server key

Parameter description

Parameter	Description
string	Text of shared password.
0* | *7	Encryption type of password, 0 indicates no encryption ; 7 indicates being simply encrypted.

Default Configuration

No specified shared password.

Command mode

Global configuration mode.

Usage guidelines

The device and TACACS+ secure server communicates with each other successfully on the basis of the shared password. Therefore, in order to make the device and TACACS+ secure server communicate with each other, the same shared password must be defined on both of them. When we need to specify different passwords to every server, use key option in **tacacs-server host** command. We can set a key to all the servers that have not set key option in global configuration mode.

Examples

The following example defines the shared password of TACACS+

secure server as aaa:

```
Ruijie(config)# tacacs-server key aaa
```

Related commands

Command	Description
tacacs-server host	Define TACACS+ secure server host.
tacacs-server timeout	Define the timeout timer of TACACS+ packet.

tacacs-server timeout

Use this command to configure the global timeout time waiting for the server when communicatin with TACACS+ server :

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter description

Parameter	Description
seconds	Timeout time (s) in the range 1 to 1000s.

Default Configuration

5s.

Command mode

Global configuration mode.

Usage guidelines

Use this command to adjust the timeout time of reply packet. When we need to specify different timeout time to every server, use timeout option in **tacacs-server host** command. We can set a timeout to all the servers that have not set timeout option in global configuration mode.

Examples

The following example shows how to define the timeout time as 10s:

```
Ruijie(config)# tacacs-server timeout 10
```

Related commands

Command	Description
tacacs-server host	Define TACACS+ secure server host.
tacacs-server key	Define the shared password of TACACS+.

debug tacacs+

Use this command to turn on the TACACS+ debugging switch. The **no** form of this command turns off the TACACS+ debugging switch.

debug tacacs+

no debug tacacs+

Parameter description N/A.

Command mode Privileged EXEC mode.

show tacacs

Use this command to show the interoperation condition with each TACACS+ server.

show tacacs

Parameter description N/A.

Default configuration N/A.

Command mode Privileged EXEC mode.

Usage guidelines Use this command to show the interoperation condition with each TACACS+ server.

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	Define TACACS+ secure server host.

host	

802.1X Configuration Commands

dot1x auth-address-table

Use this command to set the address table that can be authenticated by 802.1X. Use the **no** form of this command to delete the address table.

dot1x auth-address-table address *mac-addr* **interface** *interface*

no dot1x auth-address-table address *mac-addr* **interface** *interface*

Parameter Description

Parameter	Description
mac-addr	It specifies the physical address that can be authenticated.
interface	It specifies the interface number.

Defaults

No address can be authenticated.

Command Mode

Global configuration mode

Usage Guide

Only addresses in this table can be authenticated by 802.1X. Use the **show dot1x auth-address table** command to show the authentication address table.

Configuration Examples

The following example shows how to add an authentication address on the interface.

```
Ruijie# configure terminal
Ruijie(config)# dot1x auth-address-table address
00d0f8000000 interface ehternet 1/1
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x auth-address-table	This command is used to show the information about the address table that can be authenticated by 802.1x.

Platform Description

-

dot1x authentication

In case AAA is enabled, login must be authenticated by the AAA service. Use this command to associate login authentication method list. Use the **no** form of this command to delete the login authentication method list.

dot1x authentication {**default** | *list-name*}

no dot1x authentication {**default** | *list-name*}

Parameter Description

Parameter	Description
default	It specifies the name of the default authentication method list.
list-name	It specifies the name of the method list available.

Defaults

If AAA is enabled, the AAA service is used for login authentication by default.

Command Mode

Interface configuration mode

Usage Guide

If the AAA security service is enabled, this command is used for the login authentication with the specified method list.

Configuration Examples

The following example shows how to associate a method list on an interface and use the **group radius** for authentication.

```
Ruijie# configure terminal
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authentication dot1x default group radius
Ruijie(config)# interface fastEthernet0/1
Ruijie(config-if)# dot1x authentication default
Ruijie(config-if)# end
Ruijie#
```

Related Commands

Command	Description
aaa new-model	This command is used to enable the AAA security service.
aaa authentication dot1x	This command is used to configure the login authentication method list.

Platform Description

-

dot1x auth-fail max-attempt

Use this command to set the maximum number of failed attempts before entering VLAN.

dot1x auth-fail max-attepmt *num*

no dot1x auth-fail max-attempt

Parameter Description

Parameter	Description
num	The parameter specifies the maximum number of failed attempts before entering VLAN, and ranges from 1 to 3.

Defaults

3

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to show the setting.

Configuration Examples

The following example shows how to set the maximum number of failed attempts before entering VLAN.

```
Ruijie# configure terminal
Ruijie(config)# dot1x auth-fail max-attempt 5
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x	This command is used to show the 802.1x setting.

Platform Description

-

dot1x auth-fail vlan

Use this command to set the 802.1X authentication failure VLAN.

dot1x auth-fail vlan *vid*

no dot1x auth-fail vlan *vid*

Parameter Description

Parameter	Description
vid	It specifies the ID of the failure VLAN.

Defaults

No failure VLAN by default

Command Mode

Interface configuration mode

Usage Guide

Use the **show dot1x interface** command to show the setting.

Configuration Examples

The following example shows how to set the 802.1X authentication failure VLAN.

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# dot1x auth-fail vlan 2
Ruijie(config)# end
Ruijie#write
```

Related Commands

Command	Description

show dot1x interface	This command is used to show the 802.1x setting.

Platform Description

-

dot1x auth-mode

Use this command to set the 802.1x authentication mode.

dot1x auth-mode {**eap-md5** | **chap** | **pap**}

no dot1x auth-mode

Parameter Description

Parameter	Description
eap-md5	Use the EAP-MD5 authentication mode.
chap	Use the CHAP authentication mode.
pap	Use the PAP authentication mode.

Defaults

EAP-MD5 mode

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to show the 802.1X setting.

Configuration Examples

This example shows how to set the 802.1X authentication mode:

```
Ruijie# configure terminal
Ruijie(config)# dot1x auth-mode chap
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x	This command is used to show the 802.1x setting.

Platform Description

-

dot1x auto-req

Use this global configuration command to configure 802.1X active authentication function. Use the **no** form of this command to disable the active authentication function.

dot1x auto-req

no dot1x auto-req

Parameter Description

Parameter	Description
-	-

Defaults

Active authentication function is enabled.

Command Mode

Global configuration mode

Usage Guide

This command is used to enable active 802.1x authentication. Use the **show dot1x auto-req** command to show the setting of this function.

Configuration Examples

The following example shows how to enable active 802.1x authentication:

```
Ruijie# configure terminal
Ruijie(config)# dot1x auto-req
Ruijie(config)# end
Ruijie# show dot1x auto-req
Ruijie(config)# dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Second
```

Related Commands

Command	Description
show dot1x auto-req	The command is used to show the setting of the active authentication function.

Platform Description

-

dot1x auto-req packet-num

Use this command to set the number of authentication request messages that are actively sent by the device. Use the **no** form of this command the to apply the default setting.

dot1x auto-req packet-num *num*

no dot1x auto-req packet-num

Parameter Description

Parameter	Description
num	The parameter specifies the number of authentication request messages that are actively sent by the device.

Defaults

The default *num* is 0, that is, packets are sent continuously.

Command Mode

Global configuration mode

Usage Guide

The command is used to set the number of authentication request messages sent actively. Use the **show dot1x auto-req** command to show the setting of this function.

Configuration Examples

The following example shows how to enable a device to initiate 802.1x authentication actively and continuously:

```
Ruijie# configure terminal
Ruijie(config)# dot1x auto-req packet-num 0
Ruijie(config)# end
Ruijie# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Second
```

Related Commands

Command	Description
show dot1x auto-req	The command is used to show the setting of the active authentication function.

Platform Description

-

dot1x auto-req req-interval

Use this command to set the interval of sending authentication request messages. Use the **no** form of this command to apply the default value.

dot1x auto-req req-interval *interval*

no dot1x auto-req req-interval

Parameter Description

Parameter	Description
interval	The parameter specifies the time interval between two authentication request messages sent actively by the device, in second.

Defaults

30 seconds

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x auto-req** command to show the setting of this function.

Configuration Examples

The following example shows how to set the time interval to 60s:

```
Ruijie# configure terminal
Ruijie(config)# dot1x auto-req req-interval 60
Ruijie(config)# end
```

```
Ruijie# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 60 Second
```

Related Commands

Command	Description
show dot1x auto-req	The command is used to show the setting of the active authentication.

Platform Description

-

dot1x auto-req user-detect

Use this command to cease sending authentication request messages actively when any user passes the authentication on the device's interface. Use the **no** form of this command to apply the default setting.

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter Description

-

Defaults

Enabled

Command Mode

Global configuration mode

Usage Guide

This command is used to cease sending authentication request messages actively when any user passes the authentication on the device's interface. Use the **show dot1x auto-req** command to show the setting of this function.

Configuration Examples

The following example shows how to cease sending authentication request messages actively from an interface after a user gets online:

```
Ruijie# configure terminal
Ruijie(config)# dot1x auto-req user-detect
Ruijie(config)# end
Ruijie# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 60 Second
```

Related Commands

Command	Description

show dot1x auto-req	This command is used to show the setting of the active authentication.

Platform Description

-

dot1x client-probe enable

Use this command to enable the online probe function for the client.

dot1x client-probe enable

no dot1x client-probe enable

Parameter Description

-

Defaults

Disabled.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the online probe function for the client.

Configuration Examples

The following example shows to how to enable the online probe function for the client.

```
Ruijie# configure terminal
Ruijie(config)# dot1x client-probe enable
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:      Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        10 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          5 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Enabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description

show dot1x	The command is used to show the 802.1x setting.

Platform Description

-

dot1x critical

If all RADIUS authentication servers fail to respond and no other methods are configured in the effective 802.1x authentication method list, the user authentication fails and the network is inaccessible by default. In this case, the Inaccessible Authentication Bypass (IAB) function can be enabled on the interface to allow users to access the network.

dot1x critical

no dot1x critical

Parameter Description

Parameter	Description
-	-

Defaults

Disabled

Command Mode

Interface configuration mode

Usage Guide

After the IAB function is enabled on the interface, if only the RADIUS authentication method is configured in the 802.1x authentication method list and all RADIUS servers in this method list fail, the switch will use IAB method to authorize users to access the network and send the EAPOL-SUCCESS packet to users.

If there are other authentication methods in the 802.1x authentication method list in addition to the RADIUS authentication method, the IAB function will not be enabled. (Such as the **aaa authentication dot1x default group radius none,** there is the **none** authentication method in addition to the RADIUS authentication method.

For users authorized through IAB, if their identities cannot be authenticated, the switch will not send the accounting request no matter whether the switch is configured with the accounting function.

When the AAA multi-domain authentication is enabled globally, the 802.1x user authentication will not use the globally configured method list. Given that IAB function will send the message of successful authentication to uses directly after it confirms that all RADIUS servers in the 802.1x globally configured method list fail and does not need to enter the usernames, the AAA multi-domain authentication will fail on this interface.

Configuration Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fa 0/10
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical
Ruijie(config-if)# end
```

Related Commands

Command	Description
-	-

Platform Description

-

dot1x critical recovery action reintialize

Use this command to handle all the users that have passed the inaccessible authentication bypass on the port after the RADIUS server recovers. Use the **no** form of this command to restore the default setting.

dot1x critical recovery action reinitialize

no dot1x critical recovery action reinitialize

Parameter Description

Parameter	Description
-	-

Defaults

By default, no operation will be performed after the server recovers.

Command Mode

Interface configuration mode

Usage Guide

After the inaccessible authentication bypass function is enabled on the interface due to the server failure, when the RADIUS server recovers, the identities of all the users who have been authorized through the inaccessible authentication bypass function to access the network must be re-authenticated.

Configuration Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fa 0/10
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical recovery action reinitialize
Ruijie(config-if)# end
```

Related Commands

Command	Description
-	-

Platform Description

-

dot1x critical vlan

Use this command to configure the port to switch to the specified failed vlan when IAB is enabled. This function is disabled by default. Use the **no** form of this command to restore the default setting.

dot1x critical vlan *vlan-id*

no dot1x critical vlan

Parameter Description

Parameter	Description
vlan-id	The parameter specifies the VLAN that the port will switch to when IAB is enabled.

Defaults

Disabled

Command Mode

Interface configuration mode

Usage Guide

With this function is enabled, if no user authentication is performed on the port initially, after all RADIUS servers fail and user authentication is to be performed, IAB will be enabled on the port, which will switch to the configured VLAN. If this function is disabled, the port will not switch to the VLAN after IAB is enabled.

Configuration Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# interface fa 0/10
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x critical vlan 100
Ruijie(config-if)# end
```

Related Commands

Command	Description
-	-

Platform Description

-

dot1x default

Use this command to restore the default setting of part of the 802.1x parameters.

dot1x default

Parameter Description

-

Defaults

-

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to view the setting of 802.1X.

Configuration Examples

The following example shows how to restore the default parameters of 802.1x:

```
Ruijie# configure terminal
```

```
Ruijie(config)# dot1x default
Ruijie(config)# end
Ruijie# end
```

Related Commands

Command	Description
show dot1x	This command is used to view the setting of 802.1x.

Platform Description

-

dot1x dynamic-vlan enable

Use this command to enable dynamic VLAN switch. Use the **no** form of the command to disable the function.

dot1x dynamic-vlan enable

no dot1x dynamic-vlan enable

Parameter Description

-

Defaults

Disabled

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x dynamic-vlan** command to view the setting of 802.1X.

Configuration Examples

The following example shows how to enable dynamic VLAN switch:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 4/5
Ruijie(config-if)# dot1x dynamic-vlan enable
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x	The command is used to view the setting of the 802.1x.

Platform Description

-

dot1x eapol-tag

Use this command to enable the EAPOL frame tagging function. Use the **no** form of the command to disable the function.

dot1x eapol-tag

no dot1x eapol-tag

Parameter Description

-

Defaults

Disabled

Command Mode

Global configuration mode.

Usage Guide

Use the **show dot1x** command to view the 802.1X setting.

Configuration Examples

The following example shows how to enable the EAPOL frame tagging function:

```
Ruijie# configure terminal
Ruijie(config)# dot1x eapol-tag
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x	The command is used to view the 802.1x setting.

Platform Description

-

dot1x guest-vlan

Use this command to set whether to allow **guest vlan** jump. Use the **no** form of the command to disable the function.

dot1x guest-vlan *vid*

no dot1x guest-vlan

Parameter Description

Parameter	Description
vid	The parameter ranges from 1 to 4094.

Defaults

Disabled

Command Mode

Interface configuration mode

Usage Guide

1. Before using guest vlan, you need to configure **dot1x dynamic-vlan enable** command first.
2. When guest vlan is configured, do not modify L2 attribute of the port, especially not to add the port to a VLAN manually.
3. Use the **show running-config** command to view the 802.1x setting.

Configuration Examples

The following example shows how to set 802.1x guest vlan jumping:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 4/5
Ruijie(config-if)# dot1x guest-vlan 10
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show running-config	The command is used to view the 802.1x setting.

Platform Description

-

dot1x mac-auth-bypass

Use this command to set the MAC bypass authentication.

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Parameter Description

-

Defaults

Not supported

Command Mode

Interface configuration mode

Usage Guide

Use the **show dot1x port-control interface** command to view the setting.

Configuration Examples

The following example shows how to set the 802.1x MAC bypass authentication:

```
Ruijie# configure terminal
Ruijie(config)# interface fa 0/1
Ruijie(config)# dot1x mac-auth-bypass
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x port-control interface	The command is used to view the interface's 802.1x information.

Platform Description

-

dot1x mac-auth-bypass timeout-activity

Use this command to set the address online time for 802.1x MAC bypass authenticastion .

dot1x mac-auth-bypass timeout-activity *value*

no dot1x mac-auth-bypass timeout-activity

Parameter Description

Parameter	Description
value	The parameter specifies the online time in seconds and

	ranges between 1 and 65535.

Defaults

No default value, indicating that the address will never expire

Command Mode

Interface configuration mode

Usage Guide

Use the **show run** command to view the 802.1X setting.

Configuration Examples

The following example shows how to set the 802.1x MAC bypass authentication online time:

```
Ruijie# configure terminal
Ruijie(config)# interface fa0/1
Ruijie(config)# dot1x mac-auth-bypass timeout-activity
Ruijie(config)# end
Ruijie#write
```

Related Commands

Command	Description
show dot1x port-control interface	The command is used to show the interface's 802.1x information.

Platform Description

-

dot1x mac-auth-bypass violation

Use this command to set the 802.1x MAC bypass authentication violation.

dot1x mac-auth-bypass violation

no dot1x mac-auth-bypass violation

Parameter Description

-

Defaults

No processing for violation by default

Command Mode

Interface configuration mode.

Usage Guide

Use the **show run** command to view the 802.1X setting.

Configuration Examples

The following example shows how to set the 802.1x MAC bypass authentication violation:

```
Ruijie# configure terminal
Ruijie(config)# interface fa0/1
Ruijie(config)# dot1x mac-auth-bypass violation
Ruijie(config)# end
```

```
Ruijie#write
```

Related Commands

Command	Description
show dot1x port-control interface	The command is used to view the interface's 802.1x information.

Platform Description

-

dot1x mac-move permit

Use this command to permit a user who has passed the 802.1x authentication to move to other ports. Users are not allowed to move to other ports by default and can only access to the network from the current port.

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

dot1x mac-move permit

no dot1x mac-move permit

Parameter Description

-

Defaults

Disabled

Command Mode

Global configuration mode

Usage Guide

With this function is enabled, a user who has passed the 802.1x authentication can move to other ports. If this function is disabled, the user can not access the network after moving to the new port.

Configuration Examples

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# dot1x mac-move permit
Ruijie(config)# end
```

Related Commands

Command	Description
show dot1x	The command is used to view the 802.1x configuration.

Platform Description

-

dot1x max-req

During interaction between dot1x and a server, another request will be sent by dot1x to the server if the server fails to respond within a specified period of time. Use this command to set the maximum number of authentication requests sent to the server. Use the **no** form of the command to restore the default setting.

dot1x max-req *count*

no dot1x max-req

Parameter Description

Parameter	Description
count	The parameter specifies the maximum number of authentication requests sent to the server.

Defaults 3

Command Mode Global configuration mode

Usage Guide Use the **show dot1x** command to view the 802.1X setting.

Configuration Examples

The following example shows how to set the maximum number of authentication requests to 7:

```
Ruijie# configure terminal
Ruijie(config)# dot1x max-req 7
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x	The command is used to view the 802.1x setting.

Platform Description

-

dot1x multi-account enable

By default, users are not allowed to change their usernames to get re-authenticated after they are authenticated and get online. Use this command to allow users to change usernames. Use the **no** form of this command to restore the default setting.

dot1x multi-account enable

no dot1x multi-account enable

Parameter Description

-

Defaults

Switching to other usernames for re-authentication is not supported by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to support the application, which is needed in circumstances such as Microsoft AD domain deployment.

Configuration Examples

The following example shows how to configure multi-account switch:

```
Ruijie# configure terminal
Ruijie(config)# dot1x multi-account enable
Ruijie(config)# end
```

Related comman ds

Command	Description
show dot1x	The command is used to display the 802.1x setting.

Platform Description

-

dot1x port-control auto

In the interface configuration mode, use this command to allow the interface to be authenticated. Use the **no** form of this command to restore the default setting.

dot1x port-control auto

no dot1x port-control

Parameter Description

-

Defaults

By default, interfaces do not participate in 802.1x authentication.

Command Mode

Interface configuration mode

Usage Guide

Use the **show dot1x** command to show the 802.1X setting.

Configuration Examples

The following example shows how to set the port to participate in authentication:

```
Ruijie# configure terminal
Ruijie(config)# interface g0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# end
Ruijie#
```

Related comman ds

Command	Description
show dot1x	The command is used to view the 802.1x setting.

Platform Description

-

dot1x port-control-mode

By default, 802.1x controls users by controlling their MACs and only authenticated users have access to the network. In the port-based control mode, if one user that connects to the port passes the authentication, this port becomes an authenticated port and all users that connect to this port have access to the network. In the port-based single-user control mode, the port is authenticated when it allows only one authenticated user, who can access the network. In the port-based single-user control mode, If multiple users connect to a authenticated port, all the users on the port must be cleared and re-authenticated. The authentication mode can be configured using the following commands:

dot1x port-control-mode {**mac-based** | {**port-based [single-host]**}}

no dot1x port-control-mode

Parameter

Parameter	Description

Description

mac-based	This parameter enables the MAC address-based control mode.
port-based	This parameter enables the port-based control mode.
single-host	This parameter enables the port-based single-user control mode.

Defaults

MAC address-based control model

Command Mode

Interface configuration mode

Usage Guide

Use the **show dot1x port-control** command to view the port's 802.1X setting.
Single-host is port-based single-user 802.1x access control. The user access control will be shown as port-based on **show dot1x port-control** and dot1x port-control-mode port-based single-host on **show running-config**.
Since single-host only supports one user, manually configuration of a port as default-user-limit does not take effect in single-host mode. If the parameter default-user-limit is configured for a port when single-host is adopted, only one user can to use the network regardless of the parameter.

Configuration Examples

Example 1 shows how to set the port to participate in 802.1x authentication:

```
Ruijie(config)# interface g0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x port-control-mode
port-based
Ruijie(config-if)# end
Ruijie#
Example 2 shows how to set 802.1x single-user authentication:
Ruijie(config)# interface g 0/1
Ruijie(config-if)# dot1x port-control auto
Ruijie(config-if)# dot1x port-control-mode
port-based single-host
Ruijie(config-if)# end
Ruijie#
```

Related Commands

Command	Description
show dot1x port-control	The command is used to view the port's 802.1x setting.
Show running-config	The command is used to view the switch's setting.

dot1x private-supplicant-only

Use this command to support private clients in the global configuration mode. Use the **no** form of this command to restore to the default setting.

dot1x private-supplicant-only

no dot1x private-supplicant-only

Parameter Description

-

Defaults

Supported

Command Mode

Global configuration mode

Usage Guide

Use **show dot1x private-supplicant-only** to view the 802.1x setting.

Configuration Examples

The following example shows how to set to use private clients only:

```
Ruijie# configure t
Ruijie(config)# dot1x private-supplicant-only
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Function
show dot1x private-supplicant-only	The command is used to view the setting.

Platform Description

-

dot1x probe-timer

Use this command to enable the client probe timer.

dot1x probe-timer{**interval** | **alive**}*interval*

no dot1x probe-timer

Parameter Description

Parameter	Description
no	It restores the default setting.
interval	It specifies the interval of sending the Hello message.
alive	It specifies the alive interval.
interval	It specifies the timer value.

Defaults

The default Hello message sending interval is 20 seconds.

Default user alive interval is 250 seconds

Command Mode

Global configuration mode

Usage Guide

Configure the client-alive probe timer. Use the **show dot1x** command to view the 802.1x setting.

Configuration Examples

The following example shows how to set the Hello message sending interval to 30 seconds and the alive interval to 120 seconds:

```
Ruijie# configure terminal
Ruijie(config)# dot1x probe-timer interval 30
Ruijie(config)# dot1x probe-timer alive 120
Ruijie(config)# end
Ruijie# show dot1x probe-timer
Hello Interval: 30 Seconds
Hello Alive: 120 Seconds
```

Related Commands

Command	Description
Show dot1x probe-timer	It shows the client probe timer's configuration.

Platform Description

-

dot1x re-authentication

Use this command to require periodic re-authentication for applicants. Use the **no** form of the command to restore the default setting.

dot1x re-authentication

no dot1x re-authentication

Parameter Description

-

Defaults

Not required

Command Mode

Global configuration mode

Usage Guide

If this command is used, applicants will have to get re-authenticated periodically after they pass the authentication. Use the **show dot1x** command to show the 802.1X setting.

Configuration

The following example shows how to enables the re-authentication function:

Examples

```
Ruijie# configure terminal
Ruijie(config)# dot1x re-authentication
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:      Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        10 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	It is used to show the 802.1x setting.

Platform Description

-

dot1x reauth-max

Use this command to set the maximum number of supplicant re-authentication. Use the **no** form of the command to restore the default setting.

dot1x reauth-max *count*

no dot1x reauth-max

Parameter Description

Parameter	Description
count	It specifies the maximum number of re-authentication attempts.

Defaults

3

Command Mode

Global configuration mode

Usage Guide

Use this command to specify the maximum number of failed re-authentication attempts. Use **show dot1x** command to show the 802.1X setting.

Configuration Examples

The following example shows how to set the maximum number of re-authentication attempts:

```
Ruijie# configure terminal
Ruijie(config)# dot1x reauth-max 5
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:      Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Enable
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        10 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          5 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	It is used to show the 802.1x setting.

Platform Description

-

dot1x stationarity enable

In the port-based 802.1X control mode, dynamic users can transit freely among ports by default. This command is used to stop users from transiting from 802.1X port to other ports in special circumstances.

dot1x stationarity enable

no dot1x stationarity enable

Parameter Description

-

Defaults

Dynamic users can transit freely among ports.

Command Mode

Global configuration mode

Usage Guide

This command must be configured before user authentication. Otherwise, all users must be re-authenticated

Configuration Examples

The following example shows how to stop users from transiting from 802.1X port to other ports:

```
Ruijie# configure terminal
Ruijie(config)# dot1x stationarity enable
Ruijie(config)# end
Ruijie#
```

Related Commands

Command	Description
-	-

Platform Description

-

dot1x timeout quiet-period

Use this command to set the time (in seconds) for a device to wait for re-authentication after the authentication failure (for example, wrong authentication password). Use the **no** form of the command to restore the default setting.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameter Description

Parameter	Description
seconds	The parameter specifies the time for a device to wait for re-authentication after the authentication failure. It ranges between 0 and 65535, in seconds.

Defaults

10 seconds

Command Mode

Global configuration mode

Usage Guide

When authentication fails, the applicant must wait for a period of time before re-authentication.

Configuration Examples

The following example shows how to set the waiting time for re-authentication to 1000s:

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout quiet-period 1000
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:       Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       3600 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	It is used to view the 802.1x setting.

Platform Description

-

dot1x timeout re-authperiod

Use this command to set re-authentication interval when periodic re-authentication is enabled. Use the **no** form of the command to restore the default setting.

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Parameter Description

Parameter	Description
seconds	It specifies the re-authentication interval, ranging from 0 to 65535 seconds.

Defaults

3600 seconds

Command Mode

Global configuration mode

Usage Guide

Use **show dot1x** command to view the 802.1X setting.

Configuration Examples

The following example shows how to set the re-authentication interval to 1000s:

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout re-authperiod 1000
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:      Enabled
Authentication mode     EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	It is used to view the 802.1x setting.

Platform Description

-

dot1x timeout server-timeout

Use this command to set the authentication timeout period between a device and a authentication server. Use the **no** form of the command to restore the default setting.

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameter Description

Parameter	Description
seconds	It specifies the authentication timeout period between a device and a authentication server, ranging between 0 and 65535 seconds.

Defaults

5 seconds

Command Mode

Global configuration mode

Usage Guide

Use **show dot1x** command to view the 802.1X setting.

Configuration Examples

The following example shows how to set the authentication timeout period to 10s:

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout server-timeout 10
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:          Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         10 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	It is used to show the 802.1x setting.

Platform Description

-.

dot1x timeout supp-timeout

Use this command to set the authentication timeout between a device and applicants. Use the **no** form of the command to restore it to the default setting.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameter Description

Parameter	Description
seconds	It specifies the authentication timeout period between a device and applicants, ranging between 0 and 65535 seconds.

Defaults

3 seconds

Command Mode

Global configuration mode

Usage Guide

Use **show dot1x** command to view the 802.1X setting.

Configuration Examples

The following example shows how to set the authentication timeout period between a device and applicants to 10s:

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout supp-timeout 10
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:          Enabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	It is used to view the 802.1x setting.

Platform Description

-

dot1x timeout tx-period

Use this command to set the interval of transmitting packets after the maximum number of re-transmission times is configured. Use the **no** form of the command to restore the default setting.

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameter Description

Parameter	Description
seconds	It specifies the re-transmission interval, ranging between 0 and 65535 seconds.

Defaults

3 seconds

Command Mode

Global configuration mode

Usage Guide

Use **show dot1x** command to view the 802.1X setting.

Configuration Examples

The following example shows how to set the interval of re-transmission to 10s:

```
Ruijie# configure terminal
Ruijie(config)# dot1x timeout tx-period 10
Ruijie(config)# end
Ruijie# show dot1x
802.1X Status:      Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Disabled
Re-authen Period:       1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    10 sec
Supplicant Timeout:     10 sec
Server Timeout:         10 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	It is used to view the 802.1x setting.

Platform Description

-

show dot1x

Use this command to view 802.1x settings.

show dot1x

Parameter Description

-

Defaults

-

Command Mode

Privileged mode

Usage Guide

Configuration Examples

The following example shows how to view 802.1x settings:

```
Ruijie# show dot1x

802.1X Status:         Enabled
Authentication Mode:       EAP-MD5
Authed User Number:        0
Re-authen Enabled:         Disabled
Re-authen Period:          3600 sec
Quiet Timer Period:        10 sec
Tx Timer Period:           3 sec
Supplicant Timeout:        3 sec
Server Timeout:            5 sec
Re-authen Max:             3 times
Maximum Request:           3 times
Filter Non-RG Supp:        Disabled
Client Oline Probe:        Disabled
Eapol Tag Enable:          Disabled
Authorization Mode:        Group Server
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout	It is used to set the waiting time for re-authentication.

quiet-period	
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x auth-address-table

Use this command to display the table of 802.1Xaddresses that can be authenticated.

show dot1x auth-address-table [**address** *mac-addr*] [**interface** *interface-id*]

Parameter Description

Parameter	Description
mac-addr	It specifies the physical IP address that can be authenticated.
interface	It specifies the interface number.

Defaults

Command Mode

Privileged mode

Usage Guide

-

Configuration Examples

The following example shows how to display the table of 802.1x addresses that can be authenticated:

```
Ruijie# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac-addr 00D0.F800.0001
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description -

show dot1x auto-req

Use this command to show the configuration information of automatic 802.1x authentication.

show dot1x auto-req

Parameter Description -

Defaults -

Command Mode Privileged mode

Usage Guide -

Configuration Examples

The following example shows how to view the setting of the automatic 802.1x authentication:

```
Ruijie# show dot1x auto-req
Auto-Req: Disabled
User-Detect : Enabled
Packet-Num  : 0
Req-Interval: 30 Seconds
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x max-req

Use this command to show the maximum number of authentication request re-transmission attempts to a client.

show dot1x max-req

Parameter Description

-

Defaults

-

Command Mode

Privileged mode.

Usage Guide

-

Configuration Examples

The following example shows how to display the maximum number of authentication request re-transmission attempts:

```
Ruijie# show dot1x max-req
max-req: 2 times
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x port-control

Use this command to show ports that participate in authentication.

show dot1x port-control [**interface** *interface*]

Parameter Description

Parameter	Description
interface	It specifies the interfaces.

Defaults

-

Command Mode

Privileged mode.

Usage Guide

-

Configuration Examples

The following example shows how to view ports that participate in the authentication:

```
Ruijie# show dot1x port-control
Interface Mode      Dynamic-User Static-User Max-User Authened  Mab
---------  ----------  ------------  -----------  --------  --------
---------
Fa0/5     mac-based   0            1           6000     yes
disable
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x private-supplicant-only

Use this command to show a device's client filtering function.

show dot1x private-supplicant-only

Parameter Description

-

Defaults

-

Command Mode

Privileged mode

Usage Guide

-

Configuration Examples

The following example shows how to view the client filtering function:

```
Ruijie# show dot1x private-supplicant-only
private-supplicant-only:: disabled
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x probe-timer

Use this command to show the configuration of the client online probe timer.

show dot1x probe-timer

Parameter Description

-

Defaults

-

Command Mode

Privileged mode

Usage Guide

-

Configuration Examples

The following example shows how to view the configuration of the client online probe timer:

```
Ruijie# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x re-authentication

Use this command to show the re-authentication configuration.

show dot1x re-authentication

Parameter Description

-

Defaults

-

Command Mode

Privileged mode

Usage Guide

-

Configuration Examples

The following example shows how to view the re-authentication setting:

```
Ruijie# show dot1x re-authentication
eauth-enabled: disabled
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x reauth-max

Use this command to show the maximum number of re-authentication attempts.

show dot1x reauth-max

Parameter Description

-

Defaults

-

Command Mode

Privileged mode

Usage Guide

-

Configuration Examples

The following example shows how to view the maximum number of re-authentication attempts:

```
Ruijie# show dot1x reauth-max
reauth-max: 2 times
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x summary

Use this command to show information about the 802.1X authentication configuration table.

show dot1x summary

Parameter Description

-

Defaults

-

Command Mode

Privileged mode

Usage Guide

-

Configuration Examples

The following example shows how to display information about the 802.1x authentication configuration table:

```
Ruijie# show dot1x summary
ID       User        MAC           Interface VLAN Auth-State
Backend-State Port-Status User-Type Time
--------  ----------  --------------   ---------  ----  ---------------
------------- ----------- --------- ------------------
2       ts-user    0023.aeaa.4286  Fa0/5     1    Authenticated
Idle          Authed      static    0days 0h 8m 8s
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout	It is used to set the re-transmission interval.

tx-period	

Platform Description

-

show dot1x timeout

The following commands show 802.1X timeout information.

show dot1x timeout quiet-period

show dot1x timeout re-authperiod

show dot1x timeout server-timeout

show dot1x timeout supp-timeout

show dot1x timeout tx-period

Parameter Description

-

Defaults

-

Command Mode

Privileged mode

Usage Guide

-The command is used to view configuration of timeout parameters.

Configuration Examples

The following example shows how to view the timeout configuration:

```
Ruijie# show dot1x timeout quiet-period
quiet-period: 60 sec
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout	It is used to set the authentication timeout period between

server-timeout	a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

show dot1x user id

Use this command to view the information about the 802.1X authentication configuration table.

show dot1x user id [*id*]

Parameter Description

Parameter	Description
id	It indicates the User ID shown in show summary.

Defaults

-

Command Mode

Privileged mode

Usage Guide

-The command is used to view the information of a specific user.

Configuration Examples

The following example shows how to view the information about the 802.1x authentication configuration table:

```
Ruijie# show dot1x user id 1
User name: caikov
id: 1
Type: static
Mac address is 0013.2049.8272
Vlan id is 217
Access from port Gi0/13
User ip address is 192.168.217.64
Max user number on this port is 6000
COS on this port is 5
Up-bandwidth is 1024 kbps
Down-bandwidth is 1024 kbps
Authorization vlan is dep7
Authorization seesion time is 1000000 seconds
Authorization ip address is 192.168.217.64
Start accounting
Permit proxy user
Permit dial user
IP privilige is 2
```

```
Ruijie#
```

Related Commands

Command	Description
dot1x auth-mode	It is used to set the 802.1x authentication mode.
dot1x max-req	It is used to set the maximum number of authentication request re-transmission times.
dot1x port-control auto	It is used to set a port to participate in authentication.
dot1x reauth-max	It is used to set the maximum number of applicant re-authentication times.
dot1x re-authentication	It is used to set whether periodic re-authentication is required.
dot1x timeout quiet-period	It is used to set the waiting time for re-authentication.
dot1x timeout re-authperiod	It is used to set the re-authentication interval for an applicant.
dot1x timeout server-timeout	It is used to set the authentication timeout period between a device and authentication server.
dot1x timeout supp-timeout	It is used to set the authentication timeout period between a device and applicants.
dot1x timeout tx-period	It is used to set the re-transmission interval.

Platform Description

-

SSH Configuration Commands

crypto key generate

In global configuration mode, use this command to generate a public key on the SSH server:

crypto key generate { **rsa** | **dsa** }

Parameter Description

Parameter	Description
rsa	Generate an RSA key.
dsa	Generate a DSA key.

Defaults

By default, the SSH server does not generate a public key.

Command Mode

Global configuration mode.

Usage Guide

When you need to enable the SSH Server service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by 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.

Note

A client only adopts either a DSA or an RSA public-key algorithm to authenticate the server in one connection. But different clients support different public-key algorithms, in order to ensure clients can successfully log in to the server, it is recommended to generate both the DSA and the RSA public-key pairs on the server.

Note

The minimum length of the RSA host key and the DSA host key is 512 bits, and the maximum is 2048 bits. In SSH2, some clients (such as the SCP file transmission clients) may require the server to generate a key with the length longer than or equal to 768 bits. It is recommended to specify the modules of the host key as or larger than 768 bits when configure the RSA and DSA host keys.

Caution

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 ipssh	Show the current status of the SSH Server.
crypto key zeroize { **rsa** | **dsa** }	Delete DSA and RSA keys and disable the SSH Server function.

Platform Description

N/A.

crypto key zeroize

In global configuration mode, use this command to delete the public key on the SSH server.

crypto key zeroize { **rsa** | **dsa** }

Parameter Description

Parameter	Description
rsa	Delete the RSA key.
dsa	Delete the DSA key.

Defaults

N/A.

Command Mode

Global configuration mode.

Usage Guide

This command deletes the public key of 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 zeroizersa
```

Related Commands

Command	Description
show ipssh	Show the current status of the SSH Server.
crypto key generate { **rsa** | **dsa** }	Generate DSA and RSA keys.

Platform Description

N/A

disconnect ssh

Use this command to disconnect the established SSH session.

disconnect ssh [**vty**] *session-id*

Parameter Description

Parameter	Description
session-id	ID of the established SSH session, in the range of 0 to 35.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

You can disconnect an established SSH session by entering the ID of the SSH connection or disconnect an SSH connection by entering 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	Show the information about the established SSH connection.
clear line vty *line_number*	Disconnect the current VTY connection.

Platform Description

N/A

ip scp server enable

Use this command to enable the Secure Copy (SCP) server function on network devices. Users can directly download files from the network devices and upload local files to networks devices. All the transmitted data are in ciphertext, providing authentication and security.

ipscp server enable

no ipscp server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The SCP server function is disabled by default.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example shows how to enable the SCP function.

```
Ruijie#configure terminal
Ruijie(config)#ipscp server enable
```

Related Commands

Command	Description
show ip ssh	Display the current status information of ssh-server.

Platform Description

N/A

ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH Server. Use the **no** form of this command to restore the default setting.

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter Description

Parameter	Description
retry times	Authentication retry times, in range of 0 to 5.

Defaults

The default authentication retry times are 3. Use the **no ip ssh authentication-retries** command to restore the default value after setting other retry times.

Command Mode

Global configuration mode.

Usage Guide

User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ipssh** command to view the configuration of the SSH Server

Configuration Examples

The following example sets the authentication retry times to 2:

```
Ruijie# configure terminal
Ruijie(config)# ipssh authentication-retries 2
```

Related

Command	Description

Commands

show ipssh	Show the current status of the SSH Server.

Platform Description

N/A

ip ssh peer

Use this command to associate public-key files with user names on the client. The client can use the user name to specify a public-key file when logs in for authentication.

ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

no ipssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

Parameter Description

Parameter	Description
username	Username
filename	Public-key file name

Defaults

N/A.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example sets the associated RSA and DSA public-key files of User Test.

```
Ruijie# configure terminal
Ruijie(config)# ipssh peer test public-key rsaflash:rsa.pub
Ruijie(config)# ipssh peer test public-key dsaflash:dsa.pub
```

Related Commands

Command	Description
show ipssh	Show the current status of the SSH Server.

Platform Description

N/A

ip ssh time-out

Use this command to set the authentication timeout for the SSH Server. Use the **no** form of this command to restore the default setting.

ipssh time-out *time*

no ipssh time-out

Parameter Description

Parameter	Description
time	Authentication timeout, in range of 1 to 120s.

Defaults N/A.

Command Mode Global configuration mode.

Usage Guide The authentication is considered timeout and failed if the authentication is not successful within 120s starting from receiving a connection request. Use the **show ipssh** command to view the configuration of the SSH server.

Configuration Examples The following example sets the timeout value as 100s:

```
Ruijie# configure terminal
Ruijie(config)# ipssh time-out 100
```

Related Commands

Command	Description
show ipssh	Show 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 ipssh version

Parameter Description

Parameter	Description
1	Support the SSH1 client connection request.
2	Support the SSH2 client connection request.

Defaults SSH1 and SSH2 are compatible by default. When a version is set, the connection sent by the SSH client of this version is accepted only. The **no ipssh version** command can also be used to restore the default setting.

Command Mode Global configuration mode.

Usage Guide This command is used to configure the SSH connection protocol version supported by SSH Server.

By default, the SSH Server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH Server. Use the **show ipssh** command to show the current status of SSH Server.

Configuration Examples

The following example sets the version of the SSH Server:

```
Ruijie# configure terminal
Ruijie(config)# ipssh version 2
```

Related Commands

Command	Description
show ip ssh	Show the current status of the SSHServer.

Platform Description

N/A

show crypto key mypubkey

Use this command to show the information about the public key part of the public key on the SSH Server.

show crypto key mypubkey { **rsa | dsa** }

Parameter Description

Parameter	Description
rsa	Show the RSA key.
dsa	Show the DSA key.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

This command is used to show the information about the public key part of the generated public key on the SSH Server, including key generation time, key name, contents in the public key part.

Configuration Examples

```
Ruijie# show crypto key mypubkeyrsa
```

Related Commands

Command	Description
crypto key generate { **rsa** | **dsa** }	Generate DSA and RSA keys.

Platform Description

N/A

show ip ssh

Use this command to show the information of the SSH Server.

show ipssh

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 information of the SSH Server, including version, enablement state, authentication timeout, and authentication retry times.

If no key is generated for the SSH Server, the SSH version is still unavailable even if this SSH version has been configured.

Configuration Examples

```
Ruijie# show ip ssh
```

Related Commands

Command	Description
ip ssh version { **1** | **2** }	Configure the version for the SSH Server.
ip ssh time-out time	Set the authentication timeout for the SSH Server.
ip ssh authentication-retries	Set the authentication retry times for the SSH Server.

Platform Description

N/A

show ssh

Use this command to show the information about the SSH connection.

show ssh

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

N/A.

Command

Privileged EXEC mode.

Mode

Usage Guide

This command is used to show the information about the established SSH connections, including 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

Port-based Flow Control Configuration Commands

protected-ports route-deny

Use this command to configure the L3 routing between the protected ports. Use the **no** form of the command to disable theL3 routing.

protected-ports route-deny

no protected-ports route-deny

Default configuration

Enabled.

Command mode

Global configuration mode.

Usage guidelines

After setting some ports as the protected ports, they can route on L3. Use this command to deny the L3 communication between protected ports. Use **show running-config** to display configuration.

Examples

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

Related commands

Command	Description
show running-config	Show whether the route-deny between protected ports has been configured.

storm-control

Use this command to enable the storm suppression. Use the **no** form of the command to disable the storm suppression.

storm-control {broadcast | multicast | unicast} [{level *percent* **| pps** *packets*|*rate-bps***}]**

no storm-control {broadcast|multicast|unicast}[{level *percent* **| pps** *packets*|*rate-bps***}]**

Parameter description

Parameter	Description
broadcast	Enable the broadcast storm suppression function.
multicast	Enable the unknown unicast storm suppression function.
unicast	Enable the unknown unicast storm suppression function.

percent	According to the bandwidth percentage to set, for example, 20 means 20%
packets	According to the pps to set, which means packets per second
Rate-bps	rate allowed
64k-2M	In the unit of 64k
2-100M	in the unit of 1M
Above 100M	in the unit of 8M

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms.

A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

Use **show storm-control** to display configuration.

Examples

The following example enables the multicast storm suppression on GigabitEthernet 1/1 and sets the allowed rate to 4M.

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if)# storm-control multicast 4096
Ruijie(config-if)# end
```

Related commands

Command	Description
show storm-control	Show storm suppression information.

Platform description

switchport protected

Use this command to configure the interface as protected. Use the **no** form of the command to disable the protected port.

switchport protected

no switchport protected

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

After these ports are set as the protected ports, they cannot switch on L2 but can route on L3. A protected port can communicate with an unprotected port. Use **show interfaces** to display configuration.

Examples

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

Related commands

Command	Description
show interfaces	Show the interface information.

Platform description

For S32 and S37 series, the cross-device protected ports are not supported. ACL shall not be installed under the protected port, neither set the protected port as the controlled port since the protected port influences other security settings on the port.

switchport port-security

Use this command to configure port security and the way to deal with violation. Use the **no** form of the command to disable the port security or restore it to the default.

switchport port-security [violation {protect | restrict | shutdown}]

no switchport port-security [violation]

Parameter description

Parameter	Description
port-security	Enable interface security.
violation protect	Discard the packets breaching security.
violation restrict	Discard the packets breaching security and send the Trap message.

violation shutdown	Discard the packets breaching the security, send the Trap message and disable the interface.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.

Examples

This example shows how to enable port security on interface gigabitethernet 1/1, and the way to deal with violation is **shutdown**:

```
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security violation shutdown
```

Related commands

Command	Description
show port-security	Show port security settings.

switchport port-security aging

Use this command to set the aging time for all secure addresses on a interface. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface. Use the **no** form of the command to apply the aging time on automatically learned address or to disable the aging.

switchport port-security aging {static | time *time* }

no switchport port-security aging {static | time }

Parameter description

Parameter	Description
static	Apply the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.

time *time*	Specify the aging time for the secure address on this port. Its range is 0-1440 in minutes. If you set it to 0, the aging function is disabled actually.

Default configuration

No secure address is aged.

Command mode

Interface configuration mode.

Usage guidelines

In interface configuration mode, use **no switchport port-security aging time** to disable the aging for security addresses on the port. Use the **no switchport port-security aging static** to apply the aging time to only the dynamically learned security address.

Use **show port-security** to display configuration.

Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
```

Related commands

Command	Description
show port-security	Show port security settings.

switchport port-security binding

Use this command to configure secure address binding manually in the interface configuration mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded. Use the **no** form of the command to remove the binding addresses.

[**no**] **switchport port-security binding** *mac-address* **vlan** *vlan_id ipv4-address* | *ipv6-address*

[**no**] **switchport port-security binding** *ipv4-address* | *ipv6-address*

Parameter description

Parameter	Description
mac-address	The source MAC addresses to be bound
vlan_id	Vlan id of the binding source MAC address
ipv4-address	Binding ipv4 addresses
ipv6-address	Binding ipv6 addresses

Default configuration

N/A

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

1.This example shows how to bind the IP address *192.168.1.100* on the interface *g 0/10:*

```
Ruijie(config)#inter g0/10
Ruijie(config-if)# switchport port-security binding 192.168.1.100
```

2.This example shows how to bind the IP address *192.168.1.100* and MAC address *00d0.f800.5555 w*ith vlan id *1* on the interface *g 0/10*

```
Ruijie(config)#inter g0/10
Ruijie(config-if)# switchport port-security binding 00d0.f800.5555
vlan 1 192.168.1.100
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding interface	Configure the secure address binding in the privileged EXEC mode.
Switchport port-security mac-address	Set the static secure address.
switchport port-security aging	Set the aging time for secure address.

switchport port-security binding interface

Use this command to configure secure address binding manually in the privileged EXEC mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded. Use the **no** form of the command to remove the binding addresses

[**no**] **switchport port-security binding interface** i*nterface-id* *mac-address* **vlan** *vlan_id ipv4-address* **|** *ipv6-address*

[**no**] **switchport port-security binding interface** i*nterface-id ipv4-address* | *ipv6-address*

Parameter description

Parameter	Description
interface-id	Binding interface ID
mac-address	Binding source MAC address
Vlan_id	Vlan ID of the binding source MAC address
ipv4-address	Binding ipv4 address
ipv6-address	Binding ipv6 address

Default configuration

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

1.This example shows how to bind the IP address *192.168.1.100* on the interface *g 0/10:*

```
Ruijie(config)# switchport port-security binding interface g 0/10
192.168.1.100
```

2.This example shows how to bind the IP address *192.168.1.100* and MAC address *00d0.f800.5555 w*ith vlan id *1* on the interface *g 0/10*

```
Ruijie(config)# switchport port-security binding interface g 0/10
00d0.f800.5555 vlan 1 192.168.1.100
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding in the interface configuration mode.
switchport port-security mac-address	Set the static secure address.
switchport port-security aging	Set the aging time for secure address.

switchport port-security mac-address

Use this command to configure manually the static secure address in the interface configuration mode. Use the **no** form of the command to remove the configuration.

[no] switchport port-security mac-address mac-address [**vlan** *vlan-id*]

Parameter description

Parameter	Description
mac-address	Static secure MAC address.
vlan-id	Vlan ID of the MAC address. Note: the configuration of vlan-id is only supported on the TRUNK port.

Default configuration

N/A.

Command mode

Interface configuration mode.

Usage guidelines

N/A.

Examples

The example below describes how to configure a static secure address 00d0.f800.5555 with VID 2 for interface *g 0/10*:

```
Ruijie(config)#inter g0/10
Ruijie(config-if)# switchport port-security mac-address
00d0.f800.5555 vlan 2
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding.
switchport port-security mac-address interface	Set the static secure address in the privileged EXEC mode.
switchport port-security aging	Set the aging time for the secure address.

switchport port-security mac-address interface

Use this command to configure manually the static secure address in the privileged EXEC mode. Use the **no** form of the command to remove the configuration.

[**no**] **switchport port-security interface** i*nterface-id* **mac-address** *mac-address* [*vlan vlan-id*]

Parameter description

Parameter	Description
i*nterface-id*	Interface ID.
mac-address	Static secure address
vlan-id	Vlan ID of the MAC address. Note: the configuration of vlan-id is only supported on the TRUNK port.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The example below describes how to configure a static secure address 00d0.f800.5555 with VID 2 for interface *g 0/10*:

```
Ruijie(config)# switchport port-security interface g0/10 mac-address
00d0.f800.5555 vlan 2
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding.
Switchport port-security mac-address	Set the static secure address in the interface configuration mode.
switchport port-security aging	Set the aging time for the secure address.

switchport port-security sticky mac-address

Use this command to configure manually the Sticky MAC secure address in the interface configuration mode. Use the **no** form of the command to remove the configuration.

[**no**] **switchport port-security mac-address sticky *mac-address*** [*vlan vlan-id*]

Use the command without parameters to enable the Sticky MAC address learning. The **no** form of this command disables the Sticky MAC address learning.

[no] switchport port-security mac-address sticky

Parameter description

Parameter	Description
mac-address	Static secure address.
vlan-id	Vlan ID of the MAC address. Note: the configuration of vlan-id is only supported on the TRUNK port.

Default configuration

The Sticky MAC address learning is disabled by default.

Command mode

Interface configuration mode.

Usage guidelines

N/A.

Examples

The example below describes how to configure a static secure address 00d0.f800.5555 with VID 2 for the trunk port *g 0/10*:

```
Ruijie(config)#inter g0/10
Ruijie(config-if)# switchport port-security mac-address
00d0.f800.5555 vlan 2
```

The example below describes how to enable the Sticky MAC address learning on the interface *g0/10*：

```
Ruijie(config)#inter g0/10
Ruijie(config-if)# switchport port-security sticky mac-address
```

Related commands

Command	Description
show port-security	Show port security settings.
switchport port-security	Enable the port-security.

switchport port-security binding	Configure the secure address binding.
switchport port-security mac-address interface	Set the static secure address in the privileged EXEC mode.
switchport port-security mac-address	Set the static secure address in the interface configuration mode.
switchport port-security aging	Set the aging time for the secure address.

switchport port-security maximum

Use this command to set the maximum number of the port secure address.. Use the **no** form of the command to restore it to the default setting.

switchport port-security maximum *value*

[**no**] **switchport port-security maximum**

Parameter description

Parameter	Description
value	Maximum number of the secure address, in the range of 1 to 128.

Default configuration

128

Command mode

Interface configuration mode.

Usage guidelines

The number of the secure address contains the sum of static secure address and dynamically learnt secure address, 128 by default. If the number of the secure address you set is less than current number, it will prompt this setting failure.

Examples

The example below describes how to set the maximum number of the secure address as 2 for interface *g 0/10*

```
Ruijie(config)#inter g0/10
Ruijie(config-if)# switchport port-security maximum 2
```

Related commands

Command	Description
show port-security	Show port security settings.

switchport port-security	Enable the port-security.
switchport port-security binding	Configure the secure address binding.
Switchport port-security mac-address	Set the static secure address in the interface configuration mode.
switchport port-security aging	Set the aging time for the port secure address.

nac-author-user maximum

Use this command to set the limited number of port IP address. Use the **no** form of the command to disable the port IP address number limit.

nac-author-user maximum *value*

[**no**] **nac-author-user maximum**

Parameter description

Parameter	Description
value	The limited IP address number in the range of 1 to 1024.

Default configuration

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

If the limited number of the IP address you set is less than bound number, it will prompt this setting fails.

Examples

The example below describes how to set the limited number of the port IP address as 100

```
Ruijie(config)#inter f 0/1
Ruijie(config-if)#nac-author-user maximum 100
```

Related commands

Command	Description
show nac-author-user	Show the limited and bound number of IP address on the port.

show nac-author-user

Use this command to show the limited and bound number of IP address on the port.

show nac-auth-user

Parameter description

Parameter	Description
-	-

Default configuration All information is shown by default.

Command mode Privileged EXEC mode.

Usage guidelines N/A

Examples

```
Ruijie#show nac-author-user
```

Related commands

Command	Description
nac-auth-user maximum *value*	Set the limited number of port IP address.

show port-security

Use this command to show port security settings.

show port-security [address] [interface *interface-id***] [all]**

Parameter description

Parameter	Description
address	Show all the secure addresses or the secure address on the specified interface.
interface *interface-id*	Show the port security configuration of the specified interface.
all	Show the port security configuration of all interfaces.

Command mode Privileged EXEC mode.

Usage guidelines

This command shows all the port security configurations, secure addresses and the way to deal with violation if no parameter is configured.

Examples

```
Ruijie# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security Action
-------- -------------- ----------- -----------
Gi1/1 128 1 Restrict
Gi1/2 128 0 Restrict
Gi1/3 8 1 Protect
```

Related commands

Command	Description
switchport port-security	Enable port security and configure the way to deal with violation.
switchport port-security aging	Specify the aging time for the secure address on the interface.
switchport port-security mac-address	Configure the secure address table.

show storm-control

Use this command to show storm suppression information.

show storm-control [*interface-id*]

Parameter description

Parameter	Description
interface-id	Interface on which the storm suppression is enabled

Default configuration

All information is displayed.

Command mode

Privileged EXEC mode.

Examples

```
Ruijie# show storm-control gigabitethernet 1/1
Interface Broadcast Control Multicast Control Unicast Control
----------- --------------- ---------------- ---------------
Gi1/1 Disabled Disabled Disabled
```

Related commands

Command	Description
storm-control	Enable storm suppression.

CPU Protection Configuration Commands

cpu-protect cpu bandwidth *bandwidth_value*

Use this command to set the maximum rate for the CPU port.

cpu-protect cpu bandwidth *bandwidth_value*

Parameter description

Parameter	Description
bandwidth_value	The maximum rate for the queue, in the range of 64－1,000,000 kbps.

Default

N/A

Command mode

Global configuration mode.

Examples

The following example sets the maximum rate for the CPU port as 2000kbps:

```
Ruijie#configure terminal
Ruijie(config)# cpu-protect  cpu  bandwidth 2000
Ruijie(config)#end
Ruijie#show cpu-protect cpu
%cpu port bandwidth: 2000(kpbs)
```

Related commands

Command	Description
cpu-protect type packet-type **traffic-class** *traffic-class-num*	Set the traffic class for the corresponding packet type.
cpu-protect traffic-class id *id_num* **bandwidth** *bandwidth_value*	Set the maximum rate for each queue.
cpu-protect traffic-class all bandwidth *bandwidth_value*	Set the maximum rate for all queues.

cpu-protect mac-address storm-control enable *value*

Use this command to set the storm control for the mac-address learning.

cpu-protect mac-address storm-control enable *value*

Parameter description

Parameter	Description
value	The generated mac-address number per second, in the range of 200-51200.

Default

2000.

Command mode

Global configuration mode.

Examples

The following example sets the the maximum rate for the CPU port as 2000kbps:

```
Ruijie#configure terminal
Ruijie(config)# cpu-protect mac-address storm-control enable 3000
Ruijie(config)#end
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable
%MAC address storm control rate:  3000(address/second)
```

cpu-protect traffic-class id *id_num* bandwidth *bandwidth_value*

Use this command to set the maximum rate for each queue.

cpu-protect traffic-class id *id_num* **bandwidth** *bandwidth_value*

Parameter description

Parameter	Description
id_num	Queue id for the packet, in the range of 0-7.
bandwidth_value	The maximum rate for the queue, in the range of 32-131072kbps.

Default

N/A

Command mode

Global configuration mode.

Examples

The following example sets the the maximum rate for queue 7 as 312kbps:

```
Ruijie#configure terminal
Ruijie(config)# cpu-protect traffic-class id 7  bandwidth 312
Ruijie(config)#end
Ruijie# show cpu-protect traffic-class id 7
%*********traffic class     bandwidth(kbps)**********
             7                312
```

Related commands

Command	Description
cpu-protect type packet-type **traffic-class** *traffic-class-num*	Set the traffic class for the corresponding packet type.
cpu-protect traffic-class all bandwidth *bandwidth_value*	Set the maximum rate for all queues.
cpu-protect cpu bandwidth *bandwidth_value*	Set the maximum rate for the CPU port.

cpu-protect traffic-class all bandwidth *bandwidth_value*

Use this command to set the maximum rate for all queues.

cpu-protect traffic-class all bandwidth *bandwidth_value*

Parameter description

Parameter	Description
bandwidth_value	The maximum rate for the queue, in the range of 32-131072kbps.

Default

N/A

Command mode

Global configuration mode.

Examples

The following example sets the the maximum rate for all queues as 312kbps:

```
Ruijie#configure terminal
Ruijie(config)# cpu-protect traffic-class all  bandwidth 312
Ruijie(config)#end
```

Related commands

Command	Description
cpu-protect type packet-type **traffic-class** *traffic-class-num*	Set the traffic class for the corresponding packet type.
cpu-protect traffic-class id *id_num* **bandwidth** *bandwidth_value*	Set the maximum rate for each queue.
cpu-protect cpu bandwidth *bandwidth_value*	Set the maximum rate for the CPU port.

cpu-protect type packet-type traffic-class *traffic-class-num*

Use this command to set the traffic class for the corresponding packet type.

cpu-protect type { **bpdu | arp | tpp | dot1x | gvrp | rdlp | dhcp | unknown-ipv6-mc | known-ipv6-mc | unknown-ipv4-mc | known-ipv4-mc | udp-helper | dvmrp | igmp | icmp | ospf | pim | rip | vrrp | error-ttl | error-hop-limit | local-telnet | local-snmp | local-http | local-tftp | local-other | ipv4-uc | ipv6-uc | mld| ns | other** } **traffic-class** *traffic-class-num*

Parameter description

Parameter	Description
traffic-class-num	The corresponding queue id, in the range of 0-7.

Default

The default corresponding relationships between the packet type and queue ID are shown in the following table:

Packet Type	Queue ID
bpdu	6
arp-request	3
arp-replay	3
tpp	6
802.1x	2
gvrp	5
rldp	5
lacp	5
rerp	5
reup	5

lldp	5
dhcp	2
qinq	2
igmp	2
icmp	4
local-telnet	4
local-snmp	4
local-http	4
local-tftp	4
local-other	4
v4uc-route	0
v6uc-route	0
mld	2
nd	3
erps	5
mpls-data	0
mpls-lspv	4
web-auth	0
cfm	6
other	0

Command mode

Global configuration mode.

Examples

The following example sets the traffic class for the BPDU packet:

```
Ruijie(config)# cpu-protect type bpdu traffic-class 5
Ruijie(config)# end
Ruijie # show cpu-protect type bpdu traffic-class
%**********packet type      traffic-class**********
               bpdu           5
```

Related commands

Command	Description
cpu-protect traffic-class id *id_num* **bandwidth** *bandwidth_value*	Set the maximum rate for each queue.
cpu-protect traffic-class all bandwidth *bandwidth_value*	Set the maximum rate for all queues.
cpu-protect cpu bandwidth *bandwidth_value*	Set the maximum rate for the CPU port.

show cpu-protect cpu

Use this command to show the maximum rate for the CPU port.

show cpu-protect cpu

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the maximum rate for the CPU port.

Examples

The following example shows the maximum rate for the CPU port:

```
Ruijie# show cpu-protect cpu
%cpu port bandwidth: 100000(kbps)
```

Related commands

Command	Description
show cpu-protect type *packet-type*	Show the correponding queue for each packet type.
show cpu-protect traffic-class id *id_num*	Show the maximum rate for each queue. *id_num:* valid range is 0-7.
show cpu-protect traffic-class all	Show the maximum rate for all queues.

show cpu-protect mac-address storm-control

Use this command to show the storm control for the mac-address learning.

show cpu-protect mac-address storm-control

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the mac-address number generated per second.

Examples

The following example shows the maximum rate for the CPU port:

```
Ruijie# show cpu-protect mac-address storm-control
%MAC address storm control state: enable
%MAC address storm control rate:  2000(address/second)
```

show cpu-protect traffic-class id *id_num*

Use this command to show the maximum rate for each queue.

show cpu-protect traffic-class id *id_num*

Parameter description

Parameter	Description
id_num	In the range of 0-7.

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the maximum rate for each queue.

Examples

The following example shows the cpu protection information for queue1:

```
Ruijie#show cpu-protect traffic-class id 1

%*********traffic class     bandwidth(kbps)**********

                1               1000
```

Related commands

Command	Description
show cpu-protect type *packet-type*	Show the correponding queue for each packet type.
show cpu-protect traffic-class all	Show the maximum rate for all queues.

show cpu-protect cpu	Show the maximum rate for CPU port.

show cpu-protect traffic-class all

Use this command to show the maximum rate for all queues.

show cpu-protect traffic-class all

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the maximum rate for all queues.

Examples

The following example shows the maximum rate for all queues:

```
Ruijie# show cpu-protect traffic-class all
%*********traffic class     bandwidth(kbps)**********
            0                1000
            1                1000
            2                1000
            3                1000
            4                1000
            5                1000
            6                1000
            7                100000
```

Related commands

Command	Description
show cpu-protect type *packet-type*	Show the correponding queue for each packet type.
show cpu-protect traffic-class id *id_num*	Show the maximum rate for each queue. *id_num:* valid range is 0-7.
show cpu-protect cpu	Show the maximum rate for CPU port.

show cpu-protect type *packet-type*

Use this command to show the queue corresponding to each type of packets.

show cpu-protect type *packet-type*

Command mode

Privileged EXEC mode.

Usage guidelines

This command shows the queue corresponding to each type of packets.

Examples

The following example shows the corresponding queues of all packet types using the command **show cpu-protect type all**:

```
%**********packet type      traffic-class**********
             bpdu              6
             arp              5
              igmp              3
              dot1x             3
              gvrp              3
              dhcp              2
              unicast          4
              multicast         1
              broadcast         0
              error_ttl         0
              co-operate        6
               other             0
```

Related commands

Command	Description
show cpu-protect traffic-class id *id_num*	Show the maximum rate for each queue. *id_num:* valid range is 0-7.
show cpu-protect traffic-class all	Show the maximum rate for all queues.
show cpu-protect cpu	Show the maximum rate for CPU port.

DoS Protection Configuration Commands

ip deny invalid-tcp

Use this command to enable the anti-attack of the invalid TCP packets. Use the **no** form of this command to disable this function.

ip deny invalid-tcp

no ip deny invalid-tcp

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

N/A.

Examples

The following example shows how to enable the anti-attack of the invalid TCP packets:

```
Ruijie(config)# ip deny invalid-tcp
```

The following example shows how to disable the anti-attack of the invalid TCP packets:

```
Ruijie(config)# no ip deny invalid-tcp
```

Related commands

Command	Description
show ip deny invalid-tcp	Show the state of anti-attack of the invalid TCP packets.

ip deny land

Use this command to enable the anti-land-attack. Use the **no** form of this command to disable this function.

ip deny land

no ip deny land

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

Global configuration mode.

Usage guidelines

N/A.

Examples

The following example shows how to enable the anti-land-attack:

```
Ruijie(config)# ip deny land
```

The following example shows how to disable the anti-land-attack:

```
Ruijie(config)# no ip deny land
```

Related commands

Command	Description
show ip deny land	Show the anti-land-attack state.

show ip deny invalid-tcp

Use this command to show the state of the anti-attack of the invalid TCP packets.

show ip deny invalid-tcp

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

```
Ruijie# show ip deny invalid-tcp
DoS Protection Mode                    State
-------------------------------------  -----
protect against invalid tcp attack        On
```

Related commands

Command	Description
(**no**) **ip deny invalid-tcp**	Enable/Disable the anti-attack of the invalid TCP packets.

show ip deny land

Use this command to show the anti-land-attack state.

show ip deny land

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

```
Ruijie# show ip deny land
DoS Protection Mode             State
------------------------------      -----
protect against land attack      On
```

Related

Command	Description

commands	(**no**) **ip deny land**	Enable/Disable the anti-land-attack function.

DHCP Snooping Configuration Commands

clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP snooping binding database.

clear ip dhcp snooping binding

Parameter description

N/A.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

If users want to clear the current dynamic user information from the DHCP snooping binding database, use this command.

Examples

The following example demonstrates how to clear the dynamic database information from the DHCP snooping binding database.

```
Ruijie# clear ip dhcp snooping binding
Ruijie# show ip dhcp snooping binding
Total number of bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
---------- ---------- ---------- -------- ---- ---------
```

Related commands

Command	Description
show ip dhcp snooping binding	Show the information of the DHCP snooping binding database.

debug ip dhcp snooping

Use this command to trun on the debugging switch of the DHCP snooping.

debug ip dhcp snooping

Default

Turned off

Command mode

Privileged EXEC mode.

Examples

The following example demonstrates how to turn on the debugging switch of the DHCP snooping.

```
Ruijie# debug ip dhcp snooping
Ruijie# show ip dhcp snooping binding
```

ip dhcp snooping

Use this command to enable the DHCP snooping function globally. The **no** form of this command will disable the DHCP snooping function globally.

[**no**] **ip dhcp snooping**

Parameter description

N/A.

Default

Disabled

Command mode

Global configuration mode

Usage guidelines

Enable the DHCP snooping function on the switch. You can use the **show ip dhcp snooping** command to view whether the DHCP snooping function is enabled.

Note that DHCP Snooping cannot coexist with private VLAN.

Examples

The following is an example of enabling the DHCP snooping function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface         Trusted         Rate limit (pps)
------------------------   -------     ---------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of DHCP snooping.
ip dhcp snooping vlan	Configure DHCP snooping enabled VLAN.

ip dhcp snooping bootp-bind

Use this command to enable DHCP snooping bootp bind function. The **no** form of this command will disable the function.

[**no**] **ip dhcp snooping bootp-bind**

Parameter description

N/A.

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

By default, the DHCP Snooping only forwards Bootp packets. With this function enabled, it can snoop Bootp packets. After the Boop client requests an address successfully, the DHCP Snooping adds the Bootp user to the static binding database.

Examples

The following example enables the DHCP snooping bootp bind function.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping bootp-bind
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status :ENABLE
Verification of hwaddr field status :DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface            Trusted       Rate limit (pps)
------------------------  -------    ------------
```

Related commands

Command	Description
show ip dhcp snooping	Show the configuration of the DHCP snooping.

ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP snooping binding database into the flash periodically. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping database write-delay** *time*

Parameter

Parameter	Description

description

time	The interval at which the system writes the dynamic user information of the DHCP snooping database into the flash.

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

This function can avoid loss of user information after restart. In that case, users need to obtain IP addresses again for normal communication.

Examples

The following is an example of setting interval at which the switch writes the user information into the flash as 3600s:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: ENABLE
DHCP snooping database write-delay time: 3600
DHCP snooping option 82 status: DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface         Trusted          Rate limit (pps)
------------------------  -------     ---------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

ip dhcp snooping database write-to-flash

Parameter description

N/A.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

Examples

The following is an example of writing the dynamic user information of the DHCP binding database into flash.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
Ruijie#
```

Related commands

N/A.

ip dhcp snooping information option

Use this command to add option82 to the DHCP request message. The **no** form of this command disables this function.

[no] ip dhcp snooping information option [standard-format | dot1x-format]

Parameter description

Parameter	Description
standard-format	The option82 uses the standard format.
dot1x-format	The option82 uses the dot1x format.

Default configuration

Disabled.

Command mode

Global configuration mode.

Usage guidelines

This command adds option82 to the DHCP request message based on which the DHCP server assigns IP address.

Examples

Add option82 to the DHCP request message:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                 :   ENABLE
```

```
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time       :   0
DHCP snooping option 82 status               :   DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface             Trusted      Rate limit (pps)
------------------------ -------      ----------------
```

Related commands

Command	Function
show ip dhcp snooping	Show the configuration of the DHCP Snooping.

ip dhcp snooping information option format remote-id

Use this command to set the option82's sub-option remote-id as the customized character string. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping information option format remote-id [string** *ascii-string* **| hostname]**

Parameter description

Parameter	Description
string	The content of the option82's remote-id extension format is customized character string.
hostname	The content of the option82's remote-id extension format hostname.

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

This command sets the remote-id in the option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the option82 information.

Examples

The following is an example of adding the option82 into the DHCP request packets with the content of remote-id being hostname:

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option format
remote-id hostname
```

Related

Command	Description

commands	-	-

ip dhcp snooping suppression

Use this command to set the port to be the suppression status. The no form of this command will set the port to be no suppression status.

[**no**] **ip dhcp snooping trust**

Parameter description N/A.

Default Disabled

Command mode Interface configuration mode.

Usage guidelines This command can deny all DHCP request messages under the port, that is, all the users under the port are prohibited to request addresses through DHCP.

Examples The following is an example of setting **fastethernet** 0/2 to be suppression status:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config-if)# ip dhcp snooping suppression
Ruijie(config-if)# end
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

ip dhcp snooping trust

Use this command to set the ports of the switch as trusted ports. The no form of this command sets the ports as untrust ports.

[**no**] **ip dhcp snooping trust**

Parameter description N/A.

Default All ports are untrust ports.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to set the port as trust port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrust port will be discarded.

Examples

The following is an example of setting **fastEthernet** *0/1* as a trust port:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping trust
Ruijie(config-if)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP Snooping Support Bootp bind status:ENABLE
Interface          Trusted           Rate limit (pps)
----------------- -------          ----------------
FastEthernet0/1       yes               unlimited
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message. The **no** form of this command disables this function.

[**no**] **ip dhcp snooping verify mac-address**

Parameter description

N/A.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

Use this command to enable checking the validity of the source MAC address of the DHCP request message. Once the function is enabled, the system will discard the DHCP request message that fails to pass the source MAC address check.

Examples

The following is an example of enabling the check of the source MAC address of the DHCP request message.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
Ruijie# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
Verification of hwaddr field status: ENABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface        Trusted         Rate limit (pps)
------------------------  -------   ------------------
```

Related commands

Command	Description
show ip dhcp snooping	View the configuration information of the DHCP snooping.

ip dhcp snooping vlan

Use this command to enable DHCP snooping for the specific VLAN. The **no** form of this command will disable the DHCP snooping function for the corresponding VLAN.

[**no**] **ip dhcp snooping vlan** {*vlan-rng* **|** {*vlan-min* [*vlan-max*]}}

Parameter description

Parameter	Description
vlan-rng	VLAN range of effective DHCP snooping.
vlan-min	Minimum VLAN of effective DHCP snooping.
vlan-max	Maximum VLAN of effective DHCP snooping.

Default

By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

Command mode

Global configuration mode.

Usage guidelines

Use this command to configure effective DHCP snooping VLAN by character string.

Examples

The following example enables the DHCP snooping function in VLAN1000.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

Related commands

Command	Description
ip dhcp snooping	Global switch of DHCP snooping.

ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan

Use this command to enable the option82's sub-option circuit and change the VLAN in the circuit-id into the specified VLAN. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*

Parameter description

Parameter	Description
vlan	The specified vlan to change.

Default

Disabled

Command mode

Interface configuration mode.

Usage guidelines

With this command configured, the option82 is added to the DHCP request packets, the circuit-id in the option82 information is the specified VLAN and the DHCP server will assign the addresses according to the option82 information.

Examples

The following is an example of adding the option82 to the DHCP request packets and changing the VLAN4094 in the option82's sub-option circuit-id to VLAN93:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping vlan 4094 information option
change-vlan-to vlan 4093
Ruijie(config-if)# end
```

Related commands

Command	Description
-	-

Platform description

N/A

ip dhcp snooping vlan *vlan-id* information option format-type circuit-id string

Use this command to configure the option82's sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding. The **no** form of this command will disable this function.

[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*

Parameter description

Parameter	Description
vlan-id	The VLAN where the DHCP request packets are.
ascii-string	The user-defined content to fill to the Circuit ID.

Default

Disabled

Command mode

Interface configuration mode.

Usage guidelines

This command is used to add the option82 to the DHCP request packets. The content of the sub-option circuit-id is customized, and the DHCP server will assign the addresses according the option82 information.

Examples

The following is an example of adding the option82 to the DHCP request packets with the content of the sub-option circuit-id being *port-name*:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip dhcp snooping vlan 4094 information option
format-type circuit-id string port-name
Ruijie(config-if)# end
```

Related commands

Command	Description
-	-

Platform description

This command is supported on all switches.

renew ip dhcp snooping database

When the DHCP Snooping function is enabled, use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.

renew ip dhcp snooping database

Parameter description N/A.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is used to import the flash file information to the DHCP Snooping database in real time.

Examples The following example demonstrates how to import the flash file information to the DHCP Snooping database.

```
Ruijie# renew ip dhcp snooping database
```

Related commands

Command	Description
-	-

Platform description N/A

Related commands

Command	Description
-	-

show ip dhcp snooping

Use this command to view the setting of the DHCP snooping.

show ip dhcp snooping

Parameter description N/A.

Default N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

Show the information of DHCP Snooping.

```
Ruijie# show ip dhcp snooping
Switch DHCP snooping status :ENABLE
Verification of hwaddr field status :DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                 Trusted    Rate limit (pps)
------------------------  -------    ------------
```

Related commands

Command	Description
ip dhcp snooping	Enable the DHCP snooping globally.
ip dhcp snooping verify mac-address	Enable the check of source MAC address of DHCP Snooping packets.
ip dhcp snooping write-delay	Set the interval of writing user information to FLASH periodically.
ip dhcp snooping information option	Add option82 to the DHCP request message.
ip dhcp snoooping bootp-bind	Enable the DHCP snooping bootp bind function.
ip dhcp snooping trust	Set the port as a trust port.

show ip dhcp snooping binding

Use this command to view the information of the DHCP snooping binding database.

show ip dhcp snooping binding

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

Show the information of the DHCP Snooping binding database.

```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
```

```
MacAddress     IpAddress  Lease  Type  VLAN  Interface
00d0.f801.0101 192.168.1.1 - static 1 fastethernet 0/1
```

Related commands

Command	Description
ip dhcp snooping binding	Add the static user information to the DHCP Snooping database.
clear ip dhcp snooping binding	Clear the dynamic user information from the DHCP snooping binding database.

DAI Configuration Commands

ip arp inspection vlan *vlan-id*

Use this command to enable the DAI inspection function of the specified VLAN. The **no** option of this command disables the function of the specified VLAN. If the parameter **vlan-id** is neglected, the DAI inspection function of all VLANs will be disabled.

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan [*vlan-id*]

Parameter description

Parameter	Description
vlan-id	VLAN ID

Default

The DAI inspection function of all VLANs is disabled.

Command mode

Global configuration mode.

Usage guidelines

To execute this command, enable the DAI function firstly.

Examples

The following configuration is to check the ARP message received from VLAN 1.

```
Ruijie(config)# ip arp inspection
Ruijie(config)# ip arp inspection vlan 1
```

Related commands

Command	Description
show ip arp inspection vlan	Show the information of the DAI inspection function of the specified VLAN.

ip arp inspection trust

Use this command to configure the L2 port to a trusted port.The **no** option of this command will restore the L2 port to a untrusted port.

ip arp inspection trust

no ip arp inspection trust

Default configuration

The L2 port is a untrusted port.

Command mode

Interface configuration mode.

Usage guidelines

If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.

Examples

The configuration example below sets the gigabitEthernet 0/19 interface as the trusted port.

```
Ruijie(config)# interface gigabitEthernet 0/19
Ruijie(config-if)# ip arp inspection trust
```

Related commands

Command	Description
show ip arp inspection interface	Show related DAI information on the interface, including the trust state and rate limit of the interface.

Platform description

On the NFPP-supported switches, interface rate is limited by NFPP rather than DAI. Therefore, if you execute this command on NFPP-supported switches, only the interface trust state will be displayed.

DHCP Snooping Database Related Configuration

When the corresponding DAI funciton of the VLAN is enabled and the L2 port which receives the ARP message is configured to be a untrusted port, the validity of the ARP message is needed to check based on the DHCP Snooping database. If no configuration is carried out for the database, the ARP message passes the validity check. For the configuration on the DHCP Snooping, refer to the *DHCP Snooping Configuration*.

IP Source Guard Configuration Commands

ip source binding

Use this command to add static user information to IP source address binding database. The **no** form of this command deletes the corresponding static user:

[**no**] **ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **[interface** *interface-id* | **ip-mac | ip-only]**

Parameter description

Parameter	Description
mac-address	Add user MAC address statically.
vlan-id	Add user vlan id statically.
ip-address	Add user IP address statically.
interface-id	Add user interface id statically.
ip-mac	The global binding type is IP+MAC
ip-only	The global binding type is IP only.

Default configuration

No static binding user.

Command mode

Global configuration mode.

Examples

The following example shows how to configure a static user:

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1
interface FastEthernet 0/1
Ruijie(config)# end
Ruijie# show ip source binding
MacAddress    IpAddress  Lease(sec)   Type     VLAN  Interface
------------- --------- ----------   ----     ----  ------------
0000.0000.0001 1.1.1.1   infinite    static    1  FastEthernet 0/1
Total number of bindings: 1
```

Related commands

Command	Description
show ip source binding	View the binding information of IP source address and database.

Platform description

This command is supported on all switches.

ip verify source

Use this command to enable IP Source Guard function on the interface, The **no** form of this command disable the function.

[**no**] **ip verify source** [**port-security**]

Parameter description

Parameter	Description
port-security	Configure IP Source Guard to do IP+MAC-based detection.

Default configuration

Disabled

Command mode

Interface configuration mode.

Usage guidelines

This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection.

IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

Examples

The following example configures IP Source Guard on fastEthernet 0/1:

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ip verify source
Ruijie(config-if)# end
```

Related commands

Command	Description
show ip verify source	View user filtering entry of IP Source Guard.

Platform description

This command is supported on all switches.

show ip source binding

Use this command to view the binding information of IP source address and database.

show ip binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter description

Parameter	Description
ip-address	Show user binding information of corresponding ip.
mac-address	Show user binding information of corresponding mac.
dhcp-snooping	Show binding information of dynamic user.
static	Show binding information of static user.
vlan-id	Show user binding information of corresponding vlan.
Interface-id	Show user binding information of corresponding interface.

Default configuration

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show ip source binding static
MacAddress    IpAddress  Lease(sec)   Type     VLAN  Interface
------------- --------- ----------   ----     ----  ------------
0000.0000.0001 1.0.0.1   infinite    static    1  FastEthernet 0/1
Total number of bindings: 1
```

Related commands

Command	Description
ip source binding	Set the binding static user.

Platform description

This command is supported on all switches.

show ip verify source

Use this command to view user filtering entry of IP Source Guard.

show ip verify source [**interface** *interface-id*]

Parameter description

Parameter	Description
Interface-id	Show user filtering entry of corresponding interface.

Command mode

Privileged EXEC mode.

Usage guidelines

If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: “IP source guard is not configured on the interface FastEthernet 0/10”

Now, IP Source Guard supports the following filtering modes:

inactive-no-snooping-vlan:the interface isn’t within the range of DHCP Snooping VLAN and IP Source Guard is inactive.

inactive-trust-port :the interface is the trusted port controlled by DHCP Snooping and IP Source Guard is inactive.

Active:the interface is the untrusted port ontrolled by DHCP Snooping and IP Source Guard is active.

Examples

```
Ruijie # show ip verify source
Interface Filter-type Filter-mode Ip-address Mac-address    VLAN
--------- ----------- ----------- ---------- -------------- ----
FastEthernet 0/3   ip        active      3.3.3.3                   1
FastEthernet 0/3   ip        active      deny-all
FastEthernet 0/4    ip+mac     active        4.4.4.4    0000.0000.0001
1
FastEthernet 0/4   ip+mac    active       deny-all
```

Related commands

Command	Description
ip verify source	Set IP Source Guard on the interface.

Platform description	This command is supported on all switches.

ND Snooping Configuration Commands

ipv6 nd snooping

Use this command to enable the IPv6 ND Snooping function in global configuration mode. Use the **no** form of this command to disable this function.

ipv6 nd snooping

no ipv6 nd snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example shows how to enable the IPv6 ND Snooping function:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 nd snooping
```

Related Commands

Command	Description
show ipv6 nd snooping	Show the ipv6 nd snooping configurations.

Platform Description N/A

ipv6 nd snooping trust

Use this command to set the trust port. Use the **no** form of this command to set the untrust port.

ipv6 nd snooping trust

no ipv6 nd snooping trust

Parameter Description

Parameter	Description
N/A	N/A

Defaults The port is untrusted by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example shows how to set the interface FastEthernet 0/1 as the Trust port:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 nd snooping trust
```

Related Commands

Command	Description
show ipv6 nd snooping	Show the ipv6 nd snooping configurations.

Platform Description N/A

show ipv6 nd snooping

Use this command to show the IPv6 nd snooping static configurations.

show ipv6 nd snooping [*interface*]

Parameter Description

Parameter	Description
interface	Show the related interface configurations only.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example shows the IPv6 nd snooping static configurations:

```
Ruijie# show ipv6 mld snooping
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

DHCPv6 Snooping Configuration Commands

ipv6 dhcp snooping

Use this command to enable the DHCPv6 snooping function globally. The **no** form of this command will disable the DHCPv6 snooping function globally.

[**no**] **ipv6 dhcp snooping**

Parameter description

N/A.

Default

Disabled

Command mode

Global configuration mode

Usage guidelines

Enable the DHCPv6 snooping function on the switch. You can use the **show ip dhcpv6 snooping** command to view whether the DHCPv6 snooping function is enabled.

Examples

The following is an example of enabling the DHCPv6 snooping function.

```
Ruijie(config)# ipv6 dhcp snooping
```

Related commands

Command	Description
show ipv6 dhcp snooping	View the configuration information of DHCPv6 snooping.

Platform description

This command is supported on all switches.

ipv6 dhcp snooping binding-delay

Use this command to add the DHCPv6 snooping binding delay entry to the hardware filtering list. The **no** form of this command will disable the function.

ipv6 dhcp snooping binding-delay *seconds*

no ipv6 dhcp snooping binding-delay

Parameter description

Parameter	Description
seconds	Set the binding delay time.

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

By default, the DHCPv6 Snooping binding entries are added to the hardware filtering list. With this command configured, if no IPv6 address conflict is detected within the specified time, the DHCPv6 Snooping binding entries are added to the hardware filtering list.

Examples

```
Ruijie(config)# ipv6 dhcp snooping binding-delay 10
```

Platform description

This command is supported on all switches.

ipv6 dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCPv6 snooping binding database into the flash periodically. The **no** form of this command will disable this function.

[**no**] **ipv6 dhcp snooping database write-delay** *time*

Parameter description

Parameter	Description
time	The interval at which the system writes the dynamic user information of the DHCP snooping database into the flash.

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

This function can avoid loss of user information after restart. In that case, users need to obtain IP addresses again for normal communication.

Examples

The following is an example of setting interval at which the switch writes the user information into the flash as 100s:

```
Ruijie(config)# ip dhcp snooping database write-delay 100
```

Related commands

Command	Description
show ipv6 dhcp snooping	View the configuration information of the DHCPv6 snooping.

Platform description

This command is supported on all switches.

ipv6 dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.

ipv6 dhcp snooping database write-to-flash

Parameter description

N/A.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.

Examples

The following is an example of writing the dynamic user information of the DHCPv6 binding database into flash.

```
Ruijie(config)# ipv6 dhcp snooping database
write-to-flash
```

Platform description

This command is supported on all switches.

ipv6 dhcp snooping filter-dhcp-pkt

Use this command to filter all received DHCPv6 request packets. The **no** form of this command will disable this function.

ipv6 dhcp snooping filter-dhcp-pkt

no ipv6 dhcp snooping filter-dhcp-pkt

Parameter description	N/A.
Default	Disabled
Command mode	Interface configuration mode.
Usage guidelines	Use this command to filter all received DHCPv6 request packets, that is, to avoid all the DHCPv6 users on this interface to apply for the addresses.

Examples	The following is an example of filtering all DHCPv6 request packets on the interface fastethernet 0/1:
	`Ruijie(config)# interface fastethernet 0/1`
	`Ruijie(config-if)# ipv6 dhcp snooping filter-dhcp-pkt`

Platform description	This command is supported on all switches.

ipv6 dhcp snooping ignore dest-not-found

Use this command to ignore the destination port not found. Use the **no** form of this command to restore the DHCPv6 reply packet port check.

ipv6 dhcp snooping ignore dest-not-found

no ipv6 dhcp snooping ignore dest-not-found

Parameter description	N/A.
Default	Disabled
Command mode	Global configuration mode.

Usage guidelines

The DHCPv6 reply packet forwarding depends on the MAC address list searching. For the sake of security, the switch does not forward the related DHCPv6 reply packets if it fails to find the port of the corresponding MAC address.

However, due to the network congestion, network topology turbulance and device stack, ect, in some network, the MAC address learning delays and the it prompts `”DHCPV6_SNOOPING-5-DEST_NOT_FOUND: Could not find destination port. Destination MAC [mac-address]”.`

Examples

```
Ruijie(config)# ipv6 dhcp snooping ignore dest-not-found
```

Related commands

Command	Description
show ipv6 dhcp snooping	View the configuration information of the DHCPv6 snooping.

Platform description

This command is supported on all switches.

ipv6 dhcp snooping information option

Use this command to enable the function of adding the option18/37 into the DHCPv6 request packets. The **no** form of this command will disable this funtion.

[**no**] **ipv6 dhcp snooping information option [standard-format]**

Parameter description

Parameter	Description
standard-format	The Option18/37 uses the standard format.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

With this command configured, the option18/37 will be added to the DHCPv6 request packets and the DHCPv6 server will assign the addresses according to the option18/37 information.

Examples

The following example configures the function of adding the option18/37 into the DHCPv6 packets.

```
Ruijie# configure terminal
```

```
Ruijie(config)# ipv6 dhcp snooping information option
Ruijie(config)# end
Ruijie# show ipv6 dhcp snooping
Switch DHCPv6 snooping status : ENABLE
DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds
DHCPv6 snooping option 18/37 status: ENABLE
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 snooping link detection :DISABLE
Interface              Trusted    Filter DHCP
---------------------- -------    ---------
FastEthernet0/10          yes      DISABLE
```

Related commands

Command	Description
show ipv6 dhcp snooping	View the configuration information of the DHCPv6 snooping.

Platform description

This command is supported on all switches.

ipv6 dhcp snooping information option format remote-id

Use this command to enable the function of adding the option37 remote-id customized character string into the DHCPv6 request packets in the global configuration mode. The **no** form of this command will disable this function.

[**no**] **ipv6 dhcp snooping information option format remote-id [string** *ascii-string* **| hostname]**

Parameter description

Parameter	Description
string	The content of Option37 remote-id extension format is customized character string.
hostname	The content of Option37 remote-id extension format is hostname.

Default

Disabled.

Command mode

Global configuration mode.

Usage guidelines

With this command configured, the option37 remote-id will be added to the DHCPv6 request packets with the content being the customized and the DHCPv6 server will assign the addresses according to the option37 information.

Examples

The following example adds the option37 remote-id into the DHCPv6 request packets with the content being hostname.

```
Ruijie# configure terminal
Ruijie(config)# ipv6 dhcp snooping information option format
remote-id hostname
```

Platform description

This command is supported on all switches.

ipv6 dhcp snooping link-detection

Use this command to clear the dynamic binding entry on an interface when the interface links down. Use the **no** form of this command to disable this function.

ipv6 dhcp snooping link-detection

no ipv6 dhcp snooping link-detection

Parameter description

N/A.

Default

Disabled

Command mode

Global configuration mode.

Usage guidelines

By default, the dynamic binding entries are not cleared on an interface when the interface links down. With this function enabled, the dynamic binding entries are auto-cleared on an interface when the interface links down.

Examples

The following is an example of clearing the dynamic binding entry on an interface when the interface links down.

```
Ruijie(config)# ipv6 dhcp snooping link-detection
```

Related

Command	Description

commands

show ipv6 dhcp snooping	View the configuration information of the DHCPv6 snooping.

Platform description

This command is supported on all switches.

ipv6 dhcp snooping trust

Use this command to set the specified DHCPv6 Snooping ports as the trusted ports. The **no** form of this command sets the ports as untrust ports.

ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Parameter description

N/A.

Default

All ports are untrust ports.

Command mode

Interface configuration mode.

Usage guidelines

Use this command to set the port as trust port. The DHCPv6 Server response messages received under the trust port are forwarded normally, but the response messages received under the untrust port will be discarded.

Examples

The following is an example of setting **fastEthernet** *0/1* as a trust port:

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 dhcp snooping trust
```

Related commands

Command	Description
show ipv6 dhcp snooping	View the configuration information of the DHCPv6 snooping.

Platform description

This command is supported on all switches.

ipv6 dhcp snooping vlan

Use this command to enable DHCPv6 snooping for the specific VLAN. The **no** form of this command will disable the DHCPv6 snooping function for the corresponding VLAN.

[**no**] **ipv6 dhcp snooping vlan** {*vlan-list* **|** {*vlan-min* [*vlan-max*]}}

Parameter description

Parameter	Description
vlan-list	Set the valid VLAN range, such as 1,3-5,7,9-11.
vlan-min	Minimum VLAN ID.
vlan-max	Maximum VLAN ID.

Default

By default, once the DHCPv6 Snooping is enabled globally, it takes effect for all VLANs.

Command mode

Global configuration mode.

Usage guidelines

With the global DHCPv6 sooping enabled, this function is enabled in all VLANs by default.

Examples

The following example disables the DHCPv6 snooping function in VLAN1.

```
Ruijie(config)# no ipv6 dhcp snooping vlan 1
```

Platform description

This command is supported on all switches.

ipv6 dhcp snooping vlan vlan-id information option change-vlan-to vlan

Use this command to enable the function of adding the option18 interface-is into the DHCP request packets and change the VLAN to the specified VLAN for the forwarding . The **no** form of this command will disable this function.

[**no**] **ipv6 dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*

Parameter description

Parameter	Description
vlan-id	The specified VLAN to change.

Default

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

With this command enabled, the option18 interface-id will be added into the DHCPv6 request packets and the VLAN will be changed to the specified one and the DHCP server will assign the addresses according to the optionq8 information.

Examples

The following example adds the option18 interface-id into the DHCPv6 request packets and changes the VLAN4094 in the option to VLAN4093.

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)#  ipv6  dhcp  snooping  vlan  4094
information option change-vlan-to vlan 4093
Ruijie(config-if)# end
```

Platform description

This command is supported on all switches.

ipv6 dhcp snooping vlan vlan-id information option format-type interface-id string

Use this command to enable the function of adding the option18 into the DHCP request packets and filling the option18 interface-id with the content being the user-defined (the storage format is ASCII) and performing the packet forwarding. The **no** form of this command will disable this function.

[**no**] **ipv6 dhcp snooping vlan** *vlan-id* **information option format-type interface-id string** *ascii-string*

Parameter description

Parameter	Description
vlan-id	The VLAN where the DHCPv6 request packets are.
ascii-string	User-defined content for filling the interface-id.

Default

Disabled..

Command mode

Interface configuration mode.

Usage guidelines

With this command configured, the option18 interface-id will be added into the DHCPv6 request packets with the content being user-defined and the DHCPv6 server will assign the addresses according to the option18 information.

Examples

The following example adds the option18 interface-id into the DHCPv6 request packets with the content being *port-name*.

```
Ruijie# configure terminal
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 dhcp snooping vlan 4094 information option
format-type interface-id string port-name
Ruijie(config-if)# end
```

Platform description

This command is supported on all switches.

ipv6 source binding

Use this command to add the static binding entry for the administrator. Use the **no** form of this command to remove the static binding entries.

[no] ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* [**interface** *interface-name* **| ip-mac | ip-only]**

Parameter description

Parameter	Description
mac-address	Set the MAC address
vlan-id	Set the VLAN ID.
ipv6-address	Set the IPv6 address.
interface-name	Set the interface name.
ip-mac	The type of global binding is IP+MAC binding.
ip-only	The type of global binding is IP binding only.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

For the users using the static IPv6 address but not obtaining the IPv6 address through the DHCPv6 interaction, the administrator can add the static binding entry manually to enable the address binding on the port.

Examples

The following example shows how to add the static binding entry manually.

```
Ruijie(config)# ipv6 source binding 00d0.f866.4777 vlan 10
2001:2002::2003 interface fastethernet 0/10
```

Related commands

Command	Description
show ipv6 source binding	View all munually-added static binding entries and DHCPv6 snooping dynamic binding entries.

Platform description

This command is supported on all switches.

ipv6 verify source

Use this command to set the address binding on the interface. Use the **no** form of this command to disable the address binding.

ipv6 verify source [**port-security**]

no ipv6 verify source

Parameter description

Parameter	Description
port-security	Set the MAC address+IPV6 address filtering mode. Without this parameter, set the IPV6 address filtering mode only.

Default

Disabled

Command mode

Interface configuration mode.

Usage guidelines

With the address-binding enabled, it can prevent the user from setting the private IPv6 address, and the user can only obtain the IPv6 address through the DHCPv6 interaction, or it can manage the static binding users for the purpose of the normal communication.

Examples

The following example shows how to enable the address binding in the MAC+IPV6 filtering mode on the interface fastethernet 0/1:

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if)# ipv6 verify source port-security
```

Platform description

This command is supported on all switches.

renew ipv6 dhcp snooping database

When the DHCPv6 Snooping function is enabled, use this command to import the information in current flash to the DHCPv6 Snooping binding database manually as needed.

renew ipv6 dhcp snooping database

Parameter description

Parameter	Description
-	-

Default

Disabled

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to import the flash file information to the DHCPv6 Snooping database in real time.

Examples

The following example imports the flash file information to the DHCPv6 Snooping database.

```
Ruijie# renew ipv6 dhcp snooping database
```

Platform description

This command is supported on all switches.

show ipv6 dhcp snooping

Use this command to view the setting of the DHCPv6 snooping.

show ipv6 dhcp snooping

Parameter description

N/A.

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines N/A.

Examples

```
Ruijie# show ipv6 dhcp snooping
Switch DHCPv6 snooping status : ENABLE
DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds
DHCPv6 snooping option 18/37 status: ENABLE
DHCPv6 ignore dest-not-found :DISABLE
DHCPv6 snooping link detection :DISABLE
Interface              Trusted    Filter DHCP
----------------------  -------    ---------
FastEthernet0/10          yes      DISABLE
```

Platform description This command is supported on all switches.

show ipv6 dhcp snooping binding

Use this command to view the information of the DHCPv6 snooping binding database.

show ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan_id*] [**interface** *interface_name*]

Parameter description

Parameter	Description
ipv6-address	Show the IPv6 address binding entry.
mac-address	Show the MAC address binding entry.
vlan *vlan_id*	Show the VLAN binding entry.
interface *interface_name*	Show the interface binding entry.

Defaults N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

Show the information of the DHCP Snooping binding database.

```
Ruijie# show ipv6 dhcp snooping binding

Total number of bindings: 1

Mac Address     Ipv6 Address  Lease(s)  VLAN  Interface

-------------   ----------   -------   ----  -----------

00d0.f801.0101  2001::10     42368     2      fa 0/1
```

Platform description

This command is supported on all switches.

show ipv6 dhcp snooping prefix

Use this command to view all user information in the DHCPv6 snooping prefix list.

show ipv6 dhcp snooping prefix [*ipv6-prefix*] [*mac-address*] [**vlan** *vlan_id*] [**interface** *interface_name*]

Parameter description

Parameter	Description
ipv6-prefix	Show the IPv6 address prefix entry.
mac-address	Show the MAC address prefix entry.
vlan *vlan_id*	Show the VLAN prefix entry.
interface *interface_name*	Show the interface prefix entry.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show ipv6 dhcp snooping prefix
Total number of prefix: 1
Mac Address     IPv6 Prefix  Lease(s)  VLAN  Interface
-------------   ----------   -------   ----  -----------
00d0.f801.0101  2001:2002::/64  42368     2    fa 0/1
```

Platform description

This command is supported on all switches.

show ipv6 dhcp snooping statistics

Use this command to show the statistical information of the dhcpv6 packets.

show ipv6 dhcp snooping statistics

Parameter description

N/A.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show ipv6 dhcp snooping statistics
Packets Processed by DHCPv6 Snooping = 0
Packets Dropped Because
Received on untrusted ports     = 0
Relay forward                 = 0
No binding entry              = 0
Binding fail                  = 0
Unknown packet                = 0
Unknown output interface      = 0
No enough memory              = 0
Admin filter-dhcpv6-pkt          = 0
```

Field	Description
Received on untrusted ports	The discarded server response packets on the untrust port.

Relay forward	The packets that have been relayed once are discarded.
No binding entry	The binding entries of the release/decline packets are inexistent or error, and the packets are discarded.
Binding fail	The entry binding fails and the packets are discarded due to a lack of the hardware resources.
Unknown packet	The unknown DHCP packets.
Unknown output interface	The packets on the unknown output interface. The MAC address for the interface is not found or the trust port is not configured.
No enough memory	There is no enough memory.
Admin filter-dhcpv6-pkt	The filtered DHCPv6 packets configured by the administrator. Use the **ipv6 dhcp snooping filter-dhcp-pkt** command to filter the packets.

Platform description	This command is supported on all switches.

show ipv6 source binding

Use this command to view all static binding entry and dhcpv6 snooping dynamic binding entry.

show ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan_id*] [**interface** *interface_name*] [**dhcp-snooping | static**]

Parameter description

Parameter	Description
ipv6-prefix	Show the IPv6 address prefix entry.
mac-address	Show the MAC address prefix entry.

vlan *vlan_id*	Show the VLAN prefix entry.
interface *interface_name*	Show the interface prefix entry.
dhcp-snooping	Show the DHCPv6 snooping dynamic binding entry.
static	Show the static binding entry.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show ipv6 source binding
Total number of bindings: 1
Mac Address Ipv6 Address  Lease(s) type  Vlan   Interface
-------------   --------------  --------   ----   -----
00d0.f866.4777  2001:2002::2003  57  dynamic 10  fa 0/10
```

Platform description

This command is supported on all switches.

clear ipv6 dhcp snooping binding

Use this command to clear all the user information in the dhcpv6 snooping binding database.

clear ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan_id*] [**interface** *interface_name*]

Parameter description

Parameter	Description
ipv6-prefix	Clear the IPv6 address binding entry.
mac-address	Clear the MAC address binding entry.
vlan *vlan_id*	Clear the VLAN binding entry.
interface *interface_name*	Clear the interface binding entry.

Default

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to clear the generated user information in the dhcpv6 snooping binding database.

Examples

```
Ruijie# clear ipv6 dhcp snooping binding
```

Platform description

This command is supported on all switches.

clear ipv6 dhcp snooping prefix

Use this command to clear all the user information in the dhcpv6 snooping prefix list.

clear ipv6 dhcp snooping prefix [*ipv6-prefix*] [*mac-address*] [**vlan** *vlan_id*] [**interface** *interface_name*]

Parameter description

Parameter	Description
ipv6-prefix	Clear the IPv6 address prefix entry.
mac-address	Clear the MAC address prefix entry.
vlan *vlan_id*	Clear the VLAN prefix entry.
interface *interface_name*	Clear the interface prefix entry.

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command is used to clear the generated user information in the dhcpv6 snooping prefix list.

Examples

```
Ruijie# clear ipv6 dhcp snooping prefix
```

Platform description This command is supported on all switches.

clear ipv6 dhcp snooping statistics

Use this command to clear the statistical information of the dhcpv6 packets.

clear ipv6 dhcp snooping statistics

Parameter description

Parameter	Description
-	-

Default N/A.

Command mode Privileged EXEC mode.

Usage guidelines This command is used to clear the statistical information of the dhcpv6 packets.

Examples

```
Ruijie# clear ipv6 dhcp snooping statistics
```

Platform description This command is supported on all switches.

debug ipv6 dhcp snooping

Use this command to trurn on the debugging switch of the DHCPv6 snooping.

debug ipv6 dhcp snooping {event | packet}

no debug ipv6 dhcp snooping {event | packet}

Parameter description

Parameter	Description
event	The event debugging message. Trace the DHCPv6 SNP event processing in real time, such as the VLAN、AP change process; generating and deleting the binding entry; the switchover message of hot backup and hot plugging/ubplugging, ect.
packet	The dhcpv6 packet debugging

	messge. Trace the dhcpv6 packets in real time, such as each path action and the reason of packet drooping, ect.

Default

Turned off

Command mode

Privileged EXEC mode.

Examples

```
Ruijie# debug ipv6 dhcp snooping event
```

Platform description

This command is supported on all switches.

Anti-arp-spoofing Configuration Commands

anti-arp-spoofing ip

Use this command to enable anti-arp-spoofing. Use the **no** form of this command to disable this function.

anti-arp-spoofing ip *ip-address*

no anti-arp-spoofing ip *ip-address*

Parameter description

Parameter	Description
ip-address	IP address for the gateway.

Default

Disabled.

Command mode

Interface configuration mode.

Usage guidelines

Use the **show anti-arp-spoofing** command to view the configuration.

Examples

```
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if)#anti-arp-spoofing ip 192.168.1.1
```

Related commands

Command	Description
show anti-arp-spoofing	View the anti-arp-spoofing information on all interfaces.

show anti-arp-spoofing

Use this command to show the anti-arp-spoofing information on all interfaces.

show anti-arp-spoofing

Command mode

Privileged EXEC mode.

Examples

```
Ruijie# show anti-arp-spoofing
port                ip
Fa0/1            192.168.1.1
```

Related commands

Command	Description
anti-arp-spoofing ip	Configure the anti-arp-spoofing.

NFPP Configuration Commands

cpu-protect sub-interface {manage | protocol | route} pps

Use this command to configure the traffic bandwidth of each type of packets.

cpu-protect sub-interface {**manage** | **protocol** | **route**} **pps** *pps_vaule*

Parameter description

Parameter	Description
pps_value	The rate limit threshold, ranging from 1 to 8192

Default

The default traffic bandwidths of each type of packets are:

Manage packets: 3000pps;

Route packets: 3000pps;

Protocol packets: 3000pps.

Command mode

Global configuration mode.

Examples

```
Ruijie(config)# cpu-protect sub-interface manage pps 200
```

Related commands

Command	Description
cpu-protect sub-interface {**manage** | **protocol** | **route**} **percent**	Configure the percent value of each type of packets occupied in the buffer area.

cpu-protect sub-interface {manage | protocol | route} percent

Use this command to configure the percent value of each type of packets occupied in the buffer area.

cpu-protect sub-interface {**manage** | **protocol** | **route**} **percent** *percent_vaule*

Parameter description

Parameter	Description
percent_value	The percent value, ranging from 1 to 100.

Default	The default percent values of each type of packets occupied in the buffer area are:
	Manage packets: 30;
	Route packets: 20;
	Protocol packets: 45.

Command mode	Global configuration mode.
Examples	`Ruijie(config)# cpu-protect sub-interface manage percent 60`

Related commands

Command	Description
cpu-protect sub-interface {**manage** | **protocol** | **route**} **pps**	Configure the traffic bandwidth of each type of packets.

arp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

arp-guard attack-threshold {**per-src-ip** | **per-src-mac** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the attack threshold for each source IP address.
per-src-mac	Set the attack threshold for each source MAC address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings	By default, the attack threshold for each source IP address and source MAC address is 8pps; and the attack threshold for each port is 200pps.

Command mode

NFPP configuration mode.

Usage guidelines

The attack threshold shall be equal to or greater than the rate-limit threshold.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-mac 3
Ruijie(config-nfpp)# arp-guard attack-threshold per-port 50
```

Related commands

Command	Description
nfpp arp-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard hosts	Show the monitored host.
clear nfpp arp-guard hosts	Clear the isolated host.

arp-guard enable

Use this command to enable the anti-ARP guard function globally.

arp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Enabled.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard enable
```

Related commands

Command	Description
nfpp arp-guard enable	Enable the anti-ARP attack on the interface.
show nfpp arp-guard summary	Show the configurations.

arp-guard isolate-period

Use this command to set the arp-guard isolate time globally.

arp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard isolate-period 180
```

Related commands

Command	Description
nfpp arp-guard isolate-period	Set the isolate time on the interface.
show nfpp arp-guard summary	Show the configurations.

arp-guard monitor-period

Use this command to configure the arp guard monitor time.

arp guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

- When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
- If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitor-period 180
```

Related commands

Command	Description
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard hosts	Show the monitored host list.
clear nfpp arp-guard hosts	Clear the isolated host.

arp-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

arp-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR:The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitored-host-limit 200
```

Related commands

Command	Description
show nfpp arp-guard summary	Show the configurations.

arp-guard rate-limit

Use this command to set the arp guard rate limit.

arp-guard rate-limit {per-src-ip | per-src-mac | per-port} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate limit for each source IP address.
per-src-mac	Set the rate limit for each source MAC

	address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings

The default rate limit for each source IP address and MAC address is 4pps; the default rate limit for each port is 100pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard rate-limit per-src-ip 2
Ruijie(config-nfpp)# arp-guard rate-limit per-src-mac 3
Ruijie(config-nfpp)# arp-guard rate-limit per-port 50
```

Related commands

Command	Description
nfpp arp-guard policy	Set the rate limit and the attack threshold.
show nfpp arp-guard summary	Show the configurations.

arp-guard scan-threshold

Use this command to set the global scan threshold.

arp-guard scan-threshold *pkt-cnt*

Parameter description

Parameter	Description
pkt-cnt	Set the scan threshold, in the range of 1-9999.

Default Settings

The default scan threshold is 15, in 10 seconds.

Command mode

NFPP configuration mode.

Usage guidelines

The scanning may occur on the condition that:

more than 15 packets are received within 10 seconds;

the source MAC address for the link layer is constant while the source IP address is uncertain;

the source MAC and IP address for the link layer is constant while the destination IP address is uncertain.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard scan-threshold 20
```

Related commands

Command	Description
nfpp arp-guard scan-threshold	Set the scan threshold on the port.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard scan	Show the ARP guard scan table.
clear nfpp arp-guard scan	Clear the ARP guard scan table.

clear nfpp arp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp arp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* **|** *mac-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
ip-address	Set the IP address.
mac-address	Set the MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command without the parameter to clear all monitored hosts.

Examples

```
Ruijie# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.
nfpp arp-guard policy	Set the limit threshold and attack threshold.
show nfpp arp-guard hosts	Show the monitored host.

clear nfpp arp-guard scan

Use this command to clear ARP scanning table.

clear nfpp arp-guard scan

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# clear nfpp arp-guard scan
```

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.

nfpp arp-guard policy	Set the attack threshold.
show nfpp arp-guard scan	Show the ARP scanning table.

nfpp arp-guard enable

Use this command to enable the anti-ARP attack function on the interface.

nfpp arp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The anti-ARP attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface anti-ARP attack configuration is prior to the global configuration.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp arp-guard enable
```

Related commands

Command	Description
arp-guard enable	Enable the anti-ARP attack function.
show nfpp arp-guard summary	Show the configurations.

nfpp arp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp arp-guard isolate-period {*seconds* **| permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0

	indicates no isolation.
permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp arp-guard isolate-period 180
```

Related commands

Command	Description
arp-guard isolate-period	Set the global isolate period.
show nfpp arp-guard summary	Show the configurations.

nfpp arp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp arp-guard policy {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate-limit threshold and the attack threshold for each source IP address.
per-src-mac	Set the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Set the rate-limit threshold and the attack threshold for each port.

rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard policy per-src-ip 2 10
Ruijie(config-if)# nfpp arp-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp arp-guard policy per-port 50 100
```

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.
arp-guard rate-limit	Set the global rate-limit threshold.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard hosts	Show the monitored host.
clear nfpp arp-guard hosts	Clear the isolated host.

nfpp arp-guard scan-threshold

Use this command to set the scan threshold.

nfpp arp-guard scan-threshold *pkt-cnt*

Parameter description

Parameter	Description
pkt-cnt	Set the scan threshold with the valid range of [1, 9999].

Default Settings

By default, the sport-based scan threshold is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard scan-threshold 20
```

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.
show nfpp arp-guard summary	Show the configurations.
show nfpp arp-guard scan	Show the ARP scan table.
clear nfpp arp-guard scan	Clear the ARP scan table.

dhcp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

dhcp-guard attack-threshold { **per-src-mac** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the attack threshold for each source MAC address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The

	valid range is [1,9999].

Default Settings

By default, the attack threshold for each source MAC address is 10pps; and the attack threshold for each port is 300pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

Related commands

Command	Description
nfpp dhcp-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp dhcp-guard summary	Show the configurations.
show nfpp dhcp-guard hosts	Show the monitored host list.
clear nfpp dhcp-guard hosts	Clear the monitored host.

dhcp-guard enable

Use this command to enable the DHCP anti-attack function.

dhcp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard enable
```

dhcp-guard isolate-period

Use this command to set the isolate time globally.

dhcp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard isolate-period 180
```

Related commands

Command	Description
nfpp dhcp-guard isolate-period	Set the isolate time on the interface.
show nfpp dhcp-guard summary	Show the configurations.

dhcp-guard monitor-period

Use this command to configure the monitor time.

dhcp-guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

- When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
- If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitor-period 180
```

Related commands

Command	Description
show nfpp dhcp-guard summary	Show the configurations.
show nfpp dhcp-guard hosts	Show the monitored host list.
clear nfpp dhcp-guard hosts	Clear the isolated host.

dhcp-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

dhcp-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR:The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Related commands

Command	Description
show nfpp dhcp-guard summary	Show the configurations.

dhcp-guard rate-limit

Use this command to set the rate-limit threshold globally.

dhcp-guard rate-limit { per-src-mac | per-port} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate limit for each source MAC address.

per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings

The default rate limit for each source MAC address is 5pps; the default rate limit for each port is 150pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
Ruijie(config-nfpp)# dhcp-guard rate-limit per-port 100
```

Related commands

Command	Description
nfpp dhcp-guard policy	Set the rate limit and the attack threshold.
show nfpp dhcp-guard summary	Show the configurations.

clear nfpp dhcp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
mac-address	Set the MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command without the parameter to clear all monitored hosts.

Examples

```
Ruijie# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

Related commands

Command	Description
dhcp-guard attack-threshold	Set the global attack threshold.
nfpp dhcp-guard policy	Set the limit threshold and attack threshold.
show nfpp dhcp-guard hosts	Show the monitored host.

nfpp dhcp-guard enable

Use this command to enable the DHCP anti-attack function on the interface.

nfpp dhcp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The DHCP anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface DHCP anti- attack configuration is prior to the global configuration.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcp-guard enable
```

Related commands

Command	Description
dhcp-guard enable	Enable the anti-ARP attack function.

show nfpp dhcp-guard summary	Show the configurations.

nfpp dhcp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp dhcp-guard isolate-period {*seconds* **|** **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcp-guard isolate-period 180
```

Related commands

Command	Description
dhcp-guard isolate-period	Set the global isolate period.
show nfpp dhcp-guard summary	Show the configurations.

nfpp dhcp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp dhcp-guard policy { **per-src-mac** **|** **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Set the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp dhcp-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp dhcp-guard policy per-port 50 100
```

Related commands

Command	Description
dhcp-guard attack-threshold	Set the global attack threshold.
dhcp-guard rate-limit	Set the global rate-limit threshold.
show nfpp dhcp-guard summary	Show the configurations.
show nfpp dhcp-guard hosts	Show the monitored host.
clear nfpp dhcp-guard hosts	Clear the isolated host.

dhcpv6-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Dhcpv6-guard attack-threshold { **per-src-mac | per-port**} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the attack threshold for each source MAC address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the attack threshold for each source MAC address is 10pps; and the attack threshold for each port is 300pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

Related commands

Command	Description
nfpp dhcpv6-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp dhcpv6-guard summary	Show the configurations.
show nfpp dhcpv6-guard hosts	Show the monitored host list.
clear nfpp dhcpv6-guard hosts	Clear the monitored host.

dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function.

Dhcpv6-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Disabled

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard enable
```

dhcpv6-guard isolate-period

Use this command to set the isolate time globally.

dhcpv6-guard isolate-period {*seconds* **| permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard isolate-period 180
```

Related commands

Command	Description
nfpp dhcpv6-guard isolate-period	Set the isolate time on the interface.
show nfpp dhcpv6-guard summary	Show the configurations.

dhcpv6-guard monitor-period

Use this command to configure the monitor time.

dhcpv6-guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

- When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
- If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard monitor-period 180
```

Related

Command	Description

commands

show nfpp dhcpv6-guard summary	Show the configurations.
show nfpp dhcpv6-guard hosts	Show the monitored host list.
clear nfpp dhcpv6-guard hosts	Clear the isolated host.

dhcpv6-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

dhcpv6-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR:The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard monitored-host-limit 200
```

Related

Command	Description

commands		
	show nfpp dhcpv6-guard summary	Show the configurations.

dhcpv6-guard rate-limit

Use this command to set the rate-limit threshold globally.

dhcpv6-guard rate-limit { per-src-mac | per-port} *pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate limit for each source MAC address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings

The default rate limit for each source MAC address is 5pps; the default rate limit for each port is 150pps.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-port 100
```

Related commands

Command	Description
nfpp dhcpv6-guard policy	Set the rate limit and the attack threshold.
show nfpp dhcpv6-guard summary	Show the configurations.

clear nfpp dhcpv6-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp dhcpv6-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
mac-address	Set the MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command without the parameter to clear all monitored hosts.

Examples

```
Ruijie# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

Related commands

Command	Description
dhcpv6-guard attack-threshold	Set the global attack threshold.
nfpp dhcpv6-guard policy	Set the limit threshold and attack threshold.
show nfpp dhcpv6-guard hosts	Show the monitored host.

nfpp dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function on the interface.

nfpp dhcpv6-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The DHCPv6 anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface DHCPv6 anti- attack configuration is prior to the global configuration.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcpv6-guard enable
```

Related commands

Command	Description
dhcpv6-guard enable	Enable the anti-ARP attack function.
show nfpp dhcpv6-guard summary	Show the configurations.

nfpp dhcpv6-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp dhcpv6-guard isolate-period {*seconds* **| permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcpv6-guard isolate-period 180
```

Related commands

Command	Description
dhcpv6-guard isolate-period	Set the global isolate period.
show nfpp dhcpv6-guard summary	Show the configurations.

nfpp dhcpv6-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp dhcpv6-guard policy { **per-src-mac | per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-mac	Set the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Set the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related commands

Command	Description
dhcpv6-guard attack-threshold	Set the global attack threshold.
dhcpv6-guard rate-limit	Set the global rate-limit threshold.
show nfpp dhcpv6-guard summary	Show the configurations.
show nfpp dhcpv6-guard hosts	Show the monitored host.
clear nfpp dhcpv6-guard hosts	Clear the isolated host.

icmp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

icmp-guard attack-threshold { **per-src-ip** | **per-port**} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the attack threshold for each source IP address.
per-port	Set the attack threshold for each port.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the attack threshold and the rate-limit threshold for each source IP address and each port are the same. For the default rate-limit threshold value, see the **icmp-guard rate-limit** command.

Command mode

NFPP configuration mode.

Usage guidelines

N/A.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
Ruijie(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

Related commands

Command	Description
nfpp icmp-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp icmp-guard summary	Show the configurations.
show nfpp icmp-guard hosts	Show the monitored host list.
clear nfpp icmp-guard hosts	Clear the monitored host.

icmp-guard enable

Use this command to enable the ICMP anti-attack function.

icmp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Enabled

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard enable
```

Related commands

Command	Description
nffp icmp-guard enable	Enable the ICMP anti-attack function on the interface.
show nfpp icmp-guard summary	Show the configurations.

icmp-guard isolate-period

Use this command to set the isolate time globally.

icmp-guard isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0, or [30, 86400].
permanent	Permanent isolation.

Default Settings

The default isolate time is 0, which means no isolation.

Command mode

NFPP configuration mode.

Usage guidelines

The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard isolate-period 180
```

Related commands

Command	Description
nfpp icmp-guard isolate-period	Set the isolate time on the interface.
show nfpp icmp-guard summary	Show the configurations.

icmp-guard monitor-period

Use this command to configure the monitor time.

icmp-guard monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP configuration mode.

Usage guidelines

- When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
- If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitor-period 180
```

Related commands

Command	Description
show nfpp icmp-guard summary	Show the configurations.
show nfpp icmp-guard hosts	Show the monitored host list.
clear nfpp icmp-guard hosts	Clear the isolated host.

icmp-guard monitored-host-limit

Use this command to set the maxmum monitored host number.

icmp-guard monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR:The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to` remind the administrator.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitored-host-limit 200
```

Related commands

Command	Description
show nfpp icmp-guard summary	Show the configurations.

icmp-guard rate-limit

Use this command to set the rate-limit threshold globally.

icmp-guard rate-limit { per-src-ip | per-port} *pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate limit for each source IP address.
per-port	Set the rate limit for each port.
pps	Set the rate limit, in the range of [1,9999]

Default Settings

The default rate-limit threshold for each source IP address is half of the value for each port. And the default rate-limit threshold value for each port varies with the products:

For the IS2700G series, the default value is 400.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard rate-limit per-src-ip 500
Ruijie(config-nfpp)# icmp-guard rate-limit per-port 800
```

Related commands

Command	Description
nfpp icmp-guard policy	Set the rate limit and the attack threshold.
show nfpp icmp-guard summary	Show the configurations.

icmp-guard trusted-host

Use this command to set the trusted hosts free form monitoring.

icmp-guard trusted-host *ip mask*

no icmp-guard trusted-host {**all |** *ip mask*}

Parameter description

Parameter	Description
ip	Set the IP address.
mask	Set the IP mask.
all	Delete the configurations of all trusted hosts.

Default Settings

N/A.

Command mode

NFPP configuration mode.

Usage guidelines

The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring.

UP to 500 trusted hosts are supported.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

Related commands

Command	Description
show nfpp icmp-guard trusted-host	Show the configurations.

clear nfpp icmp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter description

Parameter	Description
vid	Set the VLAN ID.
interface-id	Set the interface name and number.
ip-address	Set the IP address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command without the parameter to clear all monitored hosts.

Examples

```
Ruijie# clear nfpp icmp-guard hosts vlan 1 interface g0/1
```

Related commands

Command	Description
icmp-guard attack-threshold	Set the global attack threshold.
nfpp icmp-guard policy	Set the limit threshold and attack threshold.
show nfpp icmp-guard hosts	Show the monitored host.

nfpp icmp-guard enable

Use this command to enable the ICMP anti-attack function on the interface.

nfpp icmp-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The ICMP anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface ICMP anti- attack configuration is prior to the global configuration.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp icmp-guard enable
```

Related commands

Command	Description
icmp-guard enable	Enable the anti-ARP attack function.
show nfpp icmp-guard summary	Show the configurations.

nfpp icmp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode.

nfpp icmp-guard isolate-period {*seconds* **| permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
permanent	Permanent isolation.

Default Settings

By default, the isolate period is not configured.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp icmp-guard isolate-period 180
```

Related commands

Command	Description
icmp-guard isolate-period	Set the global isolate period.
show nfpp icmp-guard summary	Show the configurations.

nfpp icmp-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp icmp-guard policy { **per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Set the rate-limit threshold and the attack threshold for each source IP address.
per-port	Set the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp icmp-guard policy per-src-ip 5 10
Ruijie(config-if)# nfpp icmp-guard policy per-port 100 200
```

Related commands

Command	Description
icmp-guard attack-threshold	Set the global attack threshold.
icmp-guard rate-limit	Set the global rate-limit threshold.
show nfpp icmp-guard summary	Show the configurations.
show nfpp icmp-guard hosts	Show the monitored host.
clear nfpp icmp-guard hosts	Clear the isolated host.

nd-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

nd-guard attack-threshold per-port{ **ns-na | rs | ra-redirect** } *pps*

Parameter description

Parameter	Description
ns-na	Set the neighbor request and neighbor advertisement.
rs	Set the router request.
ra-redirect	Set the router advertisement and the redirect packets.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the default attack threshold for the ns-na, rs and ra-redirect on each port is 30.

Command mode

NFPP configuration mode.

Usage guidelines

The attack threshold shall be equal to or larger than the rate-limit threshold.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Ruijie(config-nfpp)# nd-guard attack-threshold per-port rs 10
Ruijie(config-nfpp)# nd-guard attack-threshold per-port
ra-redirect 10
```

Related commands

Command	Description
nfpp ip-guard policy	Show the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Show the configurations.

nd-guard enable

Use this command to enable the ND anti-attack function.

nd-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

Enabled

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard enable
```

Related commands

Command	Description
nffp nd-guard enable	Enable the ND anti-attack function on the interface.
show nfpp nd-guard summary	Show the configurations.

nd-guard rate-limit

Use this command to set the rate-limit threshold globally.

nd-guard rate-limit per-port {**ns-na** \| **rs** \| **ra-redirect**} *pps*

Parameter description

Parameter	Description
ns-na	Set the neighbor request and neighbor advertisement.
rs	Set the router request.
ra-redirect	Set the router advertisement and the redirect packets.
pps	Set the attack threshold, in pps. The valid range is [1,9999].

Default Settings

By default, the default rate-limit threshold for the ns-na, rs and ra-redirect on each port is 15.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Ruijie(config-nfpp)# nd-guard rate-limit per-port rs 5
Ruijie(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
```

Related commands

Command	Description
nfpp nd-guard policy	Set the rate limit and the attack threshold.

show nfpp nd-guard summary	Show the configurations.

nfpp nd-guard enable

Use this command to enable the ND anti-attack function on the interface.

nfpp nd-guard enable

Parameter description

Parameter	Description
-	-

Default Settings

The ND anti-attack function is not enabled on the interface.

Command mode

Interface configuration mode.

Usage guidelines

The interface ND anti-attack configuration is prior to the global configuration.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp nd-guard enable
```

Related commands

Command	Description
nd-guard enable	Enable the ND anti- attack function.
show nfpp nd-guard summary	Show the configurations.

nfpp nd-guard policy

Use this command to set the rate-limit threshold and the attack threshold.

nfpp nd-guard policy per-port {**ns-na** | **rs** | **ra-redirect**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
ns-na	Set the neighbor request and neighbor advertisement.

rs	Set the router request.
ra-redirect	Set the router advertisement and the redirect packets.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

For ND snooping, the port is classified into untrusted port and trusted port. The untrusted port connects to the host and the trusted port connects to the gateway. The rate-limt threshold for the trusted port shall higher than the one for the untrusted port because the traffic of the trusted port generally is higher than the traffic of the untrusted port. For the trusted port with ND snooping enabled, ND snooping advertises ND guard to set the rate-limit threshold and attack threshold for the three categories of packets as 800pps and 900pps respectively.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp nd-guard policy per-port ns-na 50 100
Ruijie(config-if)# nfpp nd-guard policy per-port rs 10 20
Ruijie(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

Related commands

Command	Description
nd-guard attack-threshold	Set the global attack threshold.
nd-guard rate-limit	Set the global rate-limit threshold.
show nfpp nd-guard summary	Show the configurations.

clear nfpp define *name* hosts

Use this command to clear the monitored hosts. If the host is isolated, you need to disisolate it.

clear nfpp define *name* **hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]

Parameter description

Parameter	Description
name	Defined guard name
vid	VLAN ID
interface-id	Interface name
ip-address	IP address
ipv6-address	IPv6 address

Default Settings

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

Use this command without the parameter to clear all monitored hosts.

Examples

```
Ruijie# clear nfpp define tcp hosts vlan 1 interface g 0/1
```

Related commands

Command	Description
show nfpp define hosts	Show the isolated hosts.

define *name* enable

Use this command to enable the user-defined anti-attack globally.

define *name* **enable**

Parameter description

Parameter	Description
name	Define guard name

Default Settings

N/A

Command mode	NFPP configuration mode.

Usage guidelines	This command takes effect only after the match, rate-out, rate-limit and attack-threshold have been configured.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#define tcp enable
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

isolate-period

Use this command to set the isolate time.

isolate-period {*seconds* | **permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate time, in seconds. The valid range is 0 or [30, 86400]. 0 for no isolation.
permanent	Permanent isolation.

Default Settings	The default isolate time is 0, which means no isolation.

Command mode	NFPP define configuration mode.

Usage guidelines	If the isolate time is not 0, the host with the packets rate exceeding the attack threshold will be isolated and the packets sent by this host will be discarded.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)#isolate-period permanent
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

Platform description N/A

match

Use this command to specify the message matching filed for the user-defined anti-attack.

match [etype *type***] [src-mac** *smac* **[src-mac-mask** *smac_mask***]] [dst-mac** *dmac* **[dst-mac-mask** *dst_mask***]] [protocol** *protocol***] [src-ip** *sip* **[src-ip-mask** *sip-mask***]] [src-ipv6** *sipv6* **[src-ipv6-masklen** *sipv6-masklen***]] [dst-ip** *dip* **[dst-ip-mask** *dip-mask***]] [dst-ipv6** *dipv6* **[dst-ipv6-masklen** *dipv6-masklen***]][src-port** *sport***] [dst-port** *dport***]**

Parameter description

Parameter	Description
type	Ethernet link layer packet type
smac	Source MAC address
smac_mask	Source MAC address mask
dmac	Destination MAC address
dmac_mask	Destination MAC address mask
protocol	IPv4/v6 message protocol
sip	Source IPv4 address
sip_mask	Source IPv4 address mask
sipv6	Source IPv6 address
sipv6_masklen	Source IPv6 address mask
dip	Destination IPv4 address
dip_mask	Destination IPv4 address mask
dipv6	Destination IPv6 address
dipv6_masklen	Length of the destination IPv6 address mask.
sport	Source port

dport	Destination port

Default Settings

N/A

Command mode

NFPP configuration mode.

Usage guidelines

Use this command to create a new user-defined anti-attack type and specify the message fileds to be matched.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)#match etype 0x0800 protocol 0x06
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

monitored-host-limit

Use this command to set the maxmum monitored host number.

monitored-host-limit *number*

Parameter description

Parameter	Description
number	The maximum monitored host number. The valid range is 1-4294967295.

Default Settings

1000

Command mode

NFPP define configuration mode

Usage guidelines

If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that `%ERROR:The` `value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.` to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that `% %NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 1000 monitored hosts`. to remind the administrator.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)#monitored-host-limit 500
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

monitor period

Use this command to set the monitoring time.

monitor-period *seconds*

Parameter description

Parameter	Description
seconds	Set the monitor time, in seconds. The valid range is [180, 86400].

Default Settings

600s

Command mode

NFPP define configuration mode.

Usage guidelines

- When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
- If the isolate period has changed to be 0, the

attackers on the interface will be removed rather than being monitored by the software.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)#monitor-period 1000
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

nfpp define

Use this command to create the user-defined anti-attack type.

nfpp define *name*

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.

Default Settings

N/A

Command mode

NFPP configuration mode.

Usage guidelines

Use this command to create a new user-defined anti-attack type.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)#
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

trusted-host

Use this command to set the trusted hosts free form monitoring.

trusted-host {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}

no trusted-host {**all |** *ip mask* | *IPv6/prefixlen* }

Parameter description

Parameter	Description
ip	Set the IP address.
mac	MAC address.
mac_mask	MAC address mask.
IPv6/prefixlen	IPv6 address and mask length
mask	IP mask.
all	Delete the configurations of all trusted hosts with the **no** form of this command.

Default Settings

N/A.

Command mode

NFPP define configuration mode.

Usage guidelines

The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring.

UP to 500 trusted hosts are supported.

Before configuring the trusted-host, the match type must be configured. If the message type configured by the match is Ipv4, the Ipv6 trusted addresses are not allowed. In the same way, if the message type is IPv6, the IPv4 trusted addresses are not allowed.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
Ruijie(config-nfpp-define)#trusted-host 1.1.1.1 255.255.255.255
```

Related commands

Command	Description
show nfpp define trusted-host	Show the trusted host configurations.

global-policy

Use this command to set the rate-limit threshold and attack threshold based on the host or port.

global-policy {per-src-mac | per-src-ip | per-port} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Perform the rate statistics based on the source IP / VID and port.
per-src-mac	Perform the rate statistics based on the source MAC / VID and port.
per-port	Perform the rate statistics based on each physical port of receiving the packets.
rate-limit-pps	Set the rate-limit threshold.
attack-threshold-pps	Set the attack threshold.

Default Settings

N/A.

Command mode

NFPP define configuration mode.

Usage guidelines

To create a user-defined anti-attack type, the classification rule for the rate statistics must be specified, that is, recognize the host based on the source IP address/ source MAC address for the user-defined packets rate statistics based on the user / port and specify the rate-limit threshold and attack threshold for each classification. The rate-limit threshold shall be equal to or greater than the attack threshold. If the rate is greater than the rate-limit threshold, the packets that meet this classification rule will be discarded. If the rate exceeds the attack threshold, the user will be regarded as an attacker. The log will be printed and the trap will be sent. For the classification based on the user, the user will be isolated according to the isolate period.

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)# global-policy per-src-ip 10  20
Ruijie(config-nfpp-define)# global-policy per-port 100  200
```

Related commands

Command	Description
nfpp define *name* **policy**	Set the rate-limit threshold and attack threshold.
show nfpp define summary	Show the user-defined anti-attack configurations

nfpp define *name* enable

Use this command to enable the user-defined anti-attack function on the interface.

nfpp define *name* **enable**

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type

Default Settings

N/A

Command mode

Interface configuration mode.

Usage guidelines

This command takes effect only after the name of the user-defined anti-attack and the match, rate-count, rate-limit and the attack-threshold have been configured.

Examples

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp define tcp enable
```

Related commands

Command	Description
show nfpp define summary	Show the user-defined anti-attack configurations

nfpp define *name* isolate-period

Use this command to set the local isolate period in the interface configuration mode.

nfpp define *name* **isolate-period** {*seconds* **| permanent**}

Parameter description

Parameter	Description
seconds	Set the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
name	Name of the user-defined anti-attack type.
permanent	Permanent isolation.

Default Settings

By default, the local isolate period is not configured. The global isolate period is used.

Command mode

Interface configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp define tcp isolate-period 180
```

Related commands

Command	Description
isolate-period	Set the global isolate period.
show nfpp define summary	Show the configurations.

nfpp define *name* policy

Use this command to set the local rate-limit threshold and the attack threshold.

nfpp define *name* **policy** {**per-src-ip | per-src-mac | per-port**} *rate-limit-pps attack-threshold-pps*

Parameter description

Parameter	Description
per-src-ip	Set the attack threshold for each source IP address.
per-port	Set the attack threshold for each port.
rate-limit-pps	Set the rate-limit threshold with the valid range of [1, 9999].
attack-threshold-pps	Set the attack threshold with the valid range of [1, 9999].

Default Settings

By default, the rate-limit threshold and the attack threshold are not configured.

Command mode

Interface configuration mode.

Usage guidelines

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Examples

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp define tcp policy per-src-ip 2 10
Ruijie(config-if)# nfpp define tcp policy per-port 50 100
```

Related commands

Command	Description
define-policy	Set the global rate-limit threshold and attack threshold.
show nfpp define summary	Show the user-defined anti-attack configurations.

clear nfpp log

Use this command to clear the NFPP log buffer area.

clear nfpp log

Parameter description

Parameter	Description
-	-

Default Settings

N/A

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

```
Ruijie# clear nfpp log
32 log-buffer entries were cleared.
```

Related commands

Command	Description
show nfpp log	Show the NFPP log configurations or the log buffer area.

log-buffer entries

Use this command to set the NFPP log buffer area size.

log-buffer entries *number*

Parameter description

Parameter	Description
number	The buffer area size. The valid range is [0, 1024].

Default Settings

256.

Command mode

NFPP configuration mode.

Usage guidelines

N/A

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer entries 50
```

Related

Command	Description

commands	**log-buffer logs** number_of_message **interval** length_in_seconds	Show the rate of the syslog generated from the NFPP buffer area.
	show nfpp log	Show the NFPP log configuration or the log buffer area.

log-buffer logs

Use this command to set the rate of syslog generated from the NFPP log buffer area.

log-buffer logs *number_of_message* **interval** *length_in_seconds*

	Parameter	Description
Parameter description	*number_of_message*	The valid range is 0-1024. 0 indicates that all logs are recorded in the specific buffer area and no syslogs are generated.
	length_in_seconds	The valid range is 0-86400(one day). 0 indicates not to write the log to the buffer area but generate the syslog immediately. With both the *number_of_message* and *length_in_seconds* values are 0, it indicates not to write the log to the buffer area but generate the syslog immediately. The parameter *number_of_message /length_in_second* indicates the rate of syslog generated from the NFPP log buffer area.

Default Settings

By default, the *number_of_message is* 1 and the *length_in_seconds* is 30.

Command mode

NFPP configuration mode.

Usage

N/A

guidelines

Examples

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer logs 2 interval 12
```

Related commands

Command	Description
log-buffer entries *number*	Set the NFPP log buffer area size.
show nfpp log summary	Show the NFPP log configurations or the log buffer area.

logging

Use this command to set the VLAN or the interface log for NFPP.

logging vlan *vlan-range*

logging interface *interface-id*

Parameter description

Parameter	Description
vlan-range	Set the specified VLAN range, in the format such as “1-3, 5”.
interface-id	Set the interface ID.

Default Settings

All logs are recorded..

Command mode

NFPP configuration mode.

Usage guidelines

Use this command to filter the logs and records the logs within the specified VLAN range or the specified port.

Examples

The following example shows the administrator how to record the logs in VLAN 1,VLAN 2,VLAN 3 and VLAN 5 only:

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# logging vlan 1-3,5
```

The following example shows the administrator how to record the logs on the interface GigabitEthernet 0/1 only:

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# logging interface G 0/1
```

Related commands

Command	Description
show nfpp log summary	Show the NFPP log configurations or the log buffer area.

show nfpp log

Use this command to show the NFPP log configuration.

show nfpp log summary

Use this command to show the NFPP log buffer area content.

show nfpp log buffer [**statistics**]

Parameter description

Parameter	Description
statistics	Show the statistical information of the NFPP log buffer area.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

When the log buffer area is full, the subsequent logs are to be dropped, and an entry with all attributes ”-” is displayed in the log buffer area. The administrator shall increase the capacity of the log buffer area or improve the rate of generating the syslog.

The generated syslog in the log buffer area carries with the timestamp, for example:

```
%NFPP_ARP_GUARD-4-DOS_DETECTED:
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was
detected.(2009-07-01 13:00:00)
```

Examples

The following example shows the NFPP log configurations:

```
Ruijie#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
```

```
Logging:
  VLAN  1-3, 5
  interface Gi 0/1
  interface Gi 0/2
```

The following example shows the log number in the buffer area:

```
Ruijie#show nfpp log buffer statistics
There are 6 logs in buffer.
```

The following example shows the NFPP log buffer area:

```
Ruijie#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address    Reason
 Timestamp
------- ----  --------   ---------  -----------    ------
 ---------
ARP     1      Gi0/1      1.1.1.1     -      DoS            2009-0
5-30 16:23:10
ARP     1      Gi0/1      1.1.1.1     -      ISOLATED       2009-0
5-30 16:23:10
ARP     1      Gi0/1      1.1.1.2     -       DoS            2009-
05-30 16:23:15
ARP     1      Gi0/1      1.1.1.2     -       ISOLATE_FAILED 2009-
05-30 16:23:15
ARP     1      Gi0/1      -        0000.0000.0001  SCAN
2009-05-30 16:30:10
ARP     -      Gi0/2      -        -         PORT_ATTACKED   2009
-05-30 16:30:10
```

Field	Description
Protocol	ARP, IP, ICMP, DHCP DHCPv6, NS-NA, RS, RA-REDIRECT
Reason	1. DoS 2. ISOLATED 3. ISOLATE_FAILE 4. SCAN 5. PORT_ATTACKED

Related commands

Command	Description
clear nfpp log	Clear the NFPP log buffer area.

show nfpp arp-guard hosts

Use this command to show the monitored host.

show nfpp arp-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
Ruijie# show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120
```

The following example shows the monitored host:

```
Ruijie# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address   MAC address   remain-time(s)
----  --------   ---------   -----------   -------------
1      Gi0/1      1.1.1.1     -               110
2      Gi0/2      1.1.2.1     -               61
*3     Gi0/3      -           0000.0000.1111  110
4      Gi0/4      -           0000.0000.2222   61
Total:4 hosts
```

Related commands

Command	Description
clear nfpp arp-guard hosts	Clear the monitored host.

show nfpp arp-guard scan

Use this command to show the ARP scan list.

show nfpp arp-guard scan [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the ARP scan list.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp arp-guard scan statistics
ARP scan table has 4 record(s).


Ruijie# show nfpp arp-guard scan
VLAN   interface   IP address   MAC address    timestamp
----   --------   ----------  -----------    ---------
1      Gi0/1      N/A         0000.0000.0001   2008-01-23
16:23:10
2      Gi0/2      1.1.1.1     0000.0000.0002   2008-01-23
16:24:10
3      Gi0/3      N/A         0000.0000.0003   2008-01-23
16:25:10
4      Gi0/4      N/A         0000.0000.0004   2008-01-23
16:26:10
```

```
Total:4 record(s)


Ruijie# show nfpp arp-guard scan vlan 1 interface G 0/1
0000.0000.0001
VLAN   interface   IP address   MAC address    timestamp
----   --------    ----------   -----------    -------
1       Gi0/1      N/A          0000.0000.0001   2008-01-23
16:23:10
Total:1 record(s)
```

Related commands

Command	Description
arp-guard scan-threshold	Set the global scan threshold.
nfpp arp-guard scan-threshold	Set the scan threshold.
clear nfpp arp-guard scan	Clear the ARP scan list.

show nfpp arp-guard summary

Use this command to show the configurations.

show nfpp arp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp arp-guard summary
 Format of column Rate-limit and  Attack-threshold is per-src-ip
/per-src-mac/per-port.
Interface  Status  Isolate-period Rate-limit Attack-threshold Sc
an-threshold
Global     Enable  300            4/5/60     8/10/100         15
```

```
Gi 0/1      Enable  180            5/-/-      8/-/-
-
Gi 0/2      Disable 200            4/5/60     8/10/100         2
0

Maximum count of monitored hosts: 1000
Monitor period:300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

Related commands

Command	Description
arp-guard attack-threshold	Set the global attack threshold.
arp-guard enable	Enable the anti-ARP attack function.
arp-guard isolate-period	Set the global isolate time.
arp-guard monitor-period	Set the monitor period.
arp-guard monitored-host-limit	Set the maximum number of the monitored hosts.
arp-guard rate-limit	Set the global rate-limit threshold.
arp-guard scan-threshold	Set the global scan threshold.
nfpp arp-guard enable	Enable the anti-ARP attack function on the interface.

nfpp arp-guard isolate-period	Set the isolate time.
nfpp arp-guard policy	Set the rate-limit threshold and attack threshold.
nfpp arp-guard scan-threshold	Set the scan threshold.

show nfpp dhcp-guard hosts

Use this command to show the monitored host.

show nfpp dhcp-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
Ruijie# show nfpp dhcp-guard hosts statistics

success    fail    total

-------    ----    -----

100        20       120
```

The following example shows the monitored host:

```
Ruijie# show nfpp dhcp-guard hosts

If column 1 shows '*', it means "hardware failed to isolate host".
```

```
VLAN  interface   MAC address    remain-time(seconds)
----     ---------    -----------       -------------------
 1    gi0/2     0000.0000.0001   10
 *2    gi0/1     0000.0000.0002   20
Total:2 host(s)
```

Related commands

Command	Description
clear nfpp dhcp-guard hosts	Clear the monitored host.

show nfpp dhcp-guard summary

Use this command to show the configurations.

show nfpp dhcp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp dhcp-guard summary
 Format of column Rate-limit and  Attack-threshold is per-src-ip/
per-src-mac/per-port.
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            -/5/150    -/10/300
Gi 0/1      Enable  180            -/6/-      -/8/-
Gi 0/2      Disable 200            -/5/30    -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
```

Field	Description

Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

	Command	Description
Related commands	**dhcp-guard attack-threshold**	Set the global attack threshold.
	dhcp-guard enable	Enable the DHCP anti-attack function.
	dhcp-guard isolate-period	Set the global isolate time.
	dhcp-guard monitor-period	Set the monitor period.
	dhcp-guard monitored-host-limit	Set the maximum number of the monitored hosts.
	dhcp-guard rate-limit	Set the global rate-limit threshold.
	nfpp dhcp-guard enable	Enable the DHCP anti-attack function on the interface.
	nfpp dhcp-guard isolate-period	Set the isolate time.
	nfpp dhcp-guard policy	Set the rate-limit threshold and attack threshold.

show nfpp dhcpv6-guard hosts

Use this command to show the monitored host.

show nfpp dhcpv6-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
Ruijie# show nfpp dhcpv6-guard hosts statistics
success    fail    total
-------    ----    -----
100         20       120
```

The following example shows the monitored host:

```
Ruijie# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address    remain-time(seconds)
----    ---------    -----------        --------------------
 1     gi0/2      0000.0000.0001   10
 *2    gi0/1      0000.0000.0002   20
Total:2 host(s)
```

Related commands

Command	Description
clear nfpp dhcpv6-guard hosts	Clear the monitored host.

show nfpp dhcpv6-guard summary

Use this command to show the configurations.

show nfpp dhcpv6-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp dhcpv6-guard summary
 Format of column Rate-limit and  Attack-threshold is per-src-ip/
per-src-mac/per-port.
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            -/5/150    -/10/300
Gi 0/1      Enable  180            -/6/-      -/8/-
Gi 0/2      Disable 200            -/5/30    -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

-	No configuration.

Related commands

Command	Description
dhcpv6-guard attack-threshold	Set the global attack threshold.
dhcpv6-guard enable	Enable the DHCPv6 anti-attack function.
dhcpv6-guard isolate-period	Set the global isolate time.
dhcpv6-guard monitor-period	Set the monitor period.
dhcpv6-guard monitored-host-limit	Set the maximum number of the monitored hosts.
dhcpv6-guard rate-limit	Set the global rate-limit threshold.
nfpp dhcpv6-guard enable	Enable the DHCPv6 anti-attack function on the interface.
nfpp dhcpv6-guard isolate-period	Set the isolate time.
nfpp dhcpv6-guard policy	Set the rate-limit threshold and attack threshold.

show nfpp icmp-guard hosts

Use this command to show the monitored host.

show nfpp icmp-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
Ruijie# show nfpp icmp-guard hosts statistics

success    fail    total

-------    ----    -----

100        20       120
```

The following example shows the monitored host:

```
Ruijie# show nfpp icmp-guard hosts

If column 1 shows '*', it means "hardware failed to isolate host".

VLAN  interface IP address     remain-time(s)

----    --------   ---------         -------------

1      Gi0/1      1.1.1.1     110

2      Gi0/2      1.1.2.1     61

Total:2 host(s)
```

Related commands

Command	Description
clear nfpp icmp-guard hosts	Clear the monitored host.

show nfpp icmp-guard summary

Use this command to show the configurations.

show nfpp icmp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp icmp-guard summary
 Format of column Rate-limit and  Attack-threshold is per-src-ip/
per-src-mac/per-port.
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            4/-/60    8/-/100
Gi 0/1      Enable  180            5/-/-      8/-/-
Gi 0/2      Disable 200            4/-/60    8/-/100

Maximum count of monitored hosts: 1000
Monitor period:300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

Related commands

Command	Description
icmp-guard attack-threshold	Set the global attack threshold.
icmp-guard enable	Enable the ICMP anti-attack function.
icmp-guard isolate-period	Set the global isolate time.

icmp-guard monitor-period	Set the monitor period.
icmp-guard monitored-host-limit	Set the maximum number of the monitored hosts.
icmp-guard rate-limit	Set the global rate-limit threshold.
nfpp icmp-guard enable	Enable the ICMP anti-attack function on the interface.
nfpp icmp-guard isolate-period	Set the isolate time.
nfpp icmp-guard policy	Set the rate-limit threshold and attack threshold.

show nfpp icmp-guard trusted-host

Use this command to show the trusted host free from being monitored.

show nfpp icmp-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp icmp-guard trusted-host
IP address     mask
---------      ------
1.1.1.0       255.255.255.0
1.1.2.0       255.255.255.0
 Total:2 record(s)
```

Related

Command	Description

commands

icmp-guard trusted-host	Set the trusted host.

show nfpp ip-guard hosts

Use this command to show the monitored host.

show nfpp ip-guard hosts [**statistics** | [[*vlan vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter description

Parameter	Description
statistics	Show the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
ip-address	The IP address.
mac-address	The MAC address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The following example shows the statistical information of the monitored host:

```
Ruijie# show nfpp ip-guard hosts statistics
success   fail   total
-------   ----   -----
100        20      120
```

```
Ruijie#show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface IP address   Reason     remain-time(s)
----  --------  ---------   -------     -------------
1      Gi0/1      1.1.1.1      ATTACK      110
2      Gi0/2      1.1.2.1      SCAN         61
Total:2 host(s)
```

Related commands

Command	Description
clear nfpp ip-guard hosts	Clear the monitored host.

show nfpp ip-guard summary

Use this command to show the configurations.

show nfpp ip-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp ip-guard summary
 Format   of   column   Rate-limit   and     Attack-threshold   is
per-src-ip/per-src-mac/per-port.
Interface Status Isolate-period Rate-limit Attack-threshold Scan
-threshold
Global     Enable  300           4/-/60    8/-/100        15
Gi 0/1      Enable  180           5/-/-      8/-/-            -
Gi 0/2      Disable 200            4/-/60    8/-/100         20

Maximum count of monitored hosts: 1000
Monitor period:300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.

Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

Related commands

Command	Description
ip-guard attack-threshold	Set the global attack threshold.
ip-guard enable	Enable the IP anti-scan function.
ip-guard isolate-period	Set the global isolate time.
ip-guard monitor-period	Set the monitor period.
ip-guard monitored-host-limit	Set the maximum number of the monitored hosts.
ip-guard rate-limit	Set the global rate-limit threshold.
nfpp ip-guard enable	Enable the IP anti-scan function on the interface.
nfpp ip-guard isolate-period	Set the isolate time.
nfpp ip-guard policy	Set the rate-limit threshold and attack threshold.

show nfpp ip-guard trusted-host

Use this command to show the trusted host free from being monitored.

show nfpp ip-guard summary

Parameter description

Parameter	Description
-	-

Default Settings N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp ip-guard trusted-host
IP address     mask
---------      ------
1.1.1.0       255.255.255.0
1.1.2.0       255.255.255.0
 Total:2 record(s)
```

Related commands

Command	Description
ip-guard trusted-host	Set the trusted host.

show nfpp nd-guard trusted-host

Use this command to show the configurations.

show nfpp nd-guard summary

Parameter description

Parameter	Description
-	-

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

```
Ruijie# show nfpp nd-guard summary
 Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA
-REDIRECT.
Interface Status Rate-limit Attack-threshold
Global      Enable  20/5/10     40/10/20
Gi 0/1       Enable  15/15/15    30/30/30
Gi 0/2      Disable -/5/30      -/10/50
```

Field	Description
Interface(Global)	Global configuration
Status	Enable/Disable the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT.
Attack-threshold	In the same format as the rate-limit.
-	No configuration.

Related commands

Command	Description
nd-guard attack-threshold	Set the global attack threshold.
nd-guard enable	Enable the ND anti-attack function.
nd-guard rate-limit	Set the global rate-limit threshold.
nfpp nd-guard enable	Enable the ND anti-attack function on the interface.
nfpp nd-guard policy	Set the rate-limit threshold and attack threshold.

show nfpp define hosts

Use this command to show the monitored hosts

show nfpp define hosts *name* [**statistics |** [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.
statistics	Show the statistics of monitored hosts.
vid	Vlan ID.
interface-id	Interface name.
ip-address	IP address.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command allows filtering the hosts with parameters specified.

Examples

```
Ruijie#show nfpp define hosts tcp statistics
Define tcp:
success    fail      total
-------     ----      -----
100          20        120
```

The command execution as shown below means that there are 120 hosts monitored totally, wherein 100 hosts are isolated successfully, and 20 hosts fails.

```
Ruijie#show nfpp define hosts tcp
Define tcp:
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface    IP address  MAC address  remain-time(s)
----       --------            ---------          -------------
----------------
1      Gi0/1      1.1.1.1      -          110
2      Gi0/2      1.1.2.1      -           61
Total:2 host(s)
```

Related commands

Command	Description
clear nfpp define hosts	Clear the monitored hosts of user-defined anti-attack type.

show nfpp define summary

Use this command to show the configurations

show nfpp define summary [*name*]

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

This command can be used to show the configurations. Without the name specified, all user-defined anti-attack types will be shown.

Examples

```
Ruijie# show nfpp define summary tcp
Define tcp summary:
match etype 0x0800 protocol 0x06
Maximum count of monitored hosts: 1000
Monitor period:300s
 Format of column Rate-limit and  Attack-threshold is per-src-ip
/per-src-mac/per-port.
Interface Status Isolate-period Rate-limit Attack-threshold
Global     Enable  300           -/5/150    -/10/300
G 0/1      Enable  180           -/6/-      -/8/-
G 0/2      Disable 200           -/5/30    -/10/50
```

Field	Description
Interface	If the interface field is shown as Global, it means that is configured in the global configuration mode.
Status	Enable/ Disable the anti-attack function.

Related commands

Command	Description
match	Clear the monitored hosts of user-defined anti-attack type.
policy	Attack threshold and rate-limit threshold.
isolate-period	Isolate time
monitored-period	Monitored time
monitored-host-limit	Maximum monitored host number

show nfpp define trusted-host

Use this command to show the trusted host free from monitoring.

show nfpp define trusted-host *name*

Parameter description

Parameter	Description
name	Name of the user-defined anti-attack type.

Default Settings

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A

Examples

The following example shows the trusted host configurations.

```
Ruijie# show nfpp define trusted-host tcp
Define tcp:
IP address     mask
---------      ------
1.1.1.0       255.255.255.0
1.1.2.0       255.255.255.0
Total:2 record(s)
```

Related commands

Command	Description
trusted-host	Configure the trusted hosts.

ACL&QoS Configuration Commands

1. ACL Configuration Commands
2. QoS Configuration Commands

ACL Configuration Commands

command ID table

For IDs used in the following commands, refer to the command ID table below:

ID	Meaning
ID	Number of access list. Range: Standard IP ACL: 1 to 99, 1300 to 1999 Extended IP ACL: 100 to 199,2000 to 2699 Extended MAC ACL: 700 to 799 Extended expert ACL: 2700 to 2899
name	ACL name
sn	ACL SN (products can be set according to the priority)
start-sn	Start sequence number
inc-sn	Sequence number increment
deny	If matched, access is denied.
permit	If matched, access is permitted.
port	Protocol number. For IPv6, this field can be IPv6, icmp, tcp, udp and numbers 0 to 255. For IPv4, it can be one of eigrp, gre, ipinip, igmp, nos, ospf, icmp, udp, tcp, esp, pcp, pim and ip, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as icmp/tcp/udp, are listed individually.
interface *idx*	Interface index
src	Packet source IP address (host address or network address)
src-wildcard	Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.
src-ipv6-pfix	Source IPv6 network address or network type
dst-ipv6-pfix	Destination IPv6 network address or network type
pfix-len	Prefix mask length
src-ipv6-addr	Source IPv6 address
dst-ipv6-addr	Destination IPv6 address
dscp	Differential service code point, and code point value. Range: 0 to 63
flow-label	Flow label in the range 0 to 1,048,575
dst	Packet destination IP address (host address or network address)
dst-wildcard	Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32
fragment	Packet fragment filtering.

precedence	Packet precedence value (0 to 7)
range	The layer 4 port number range of the packet.
time-range tm-rng-name	Time range of packet filtering, named *tm-rng-name*
tos	Type of service (0 to 15)
cos	Class of service (0-7)
cos inner *cos*	COS of the packet tag
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name (0 to 255)
operator port[port]	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range) *port* indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number
src-mac-addr	Physical address of the source host
dst-mac-addr	Physical address of the destination host
VID vid	VLAN ID
VID inner vid	VID of the tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all *tcpf*	Match all bits of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{rule mask offset}$^+$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table “+” sign indicates at least one group
log	Output the matching syslog when the packet matches the ACL rule.

The fields in the packet are as follows:

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

The corresponding offset table is as follows:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol number	35
C	Data frame length field	12	Q	IP check sum	36

D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version number	26	XY	IP header length and reserved bits	58
K	TOS field	27	Z	Resrved bits and flags bit	59
L	Length of IP packet	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

The offsets of fields in the above table are their offsets in 802.3 data frames of SNAP+tag.

access-list

Use this command to create an access list rule to filter data packets. The **no** form of this command deletes the specified access list entries.

Standard IP access list (1 to 99, 1300 to 1999)

access-list *id* { **deny** | **permit** } { *source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*] [**log**]

Extended IP access list (100 to 199, 2000 to 2699)

access-list *id* {**deny** | **permit**} **protocol** {*source source-wildcard* | **host** *source* | **any| interface** *idx* } {*destination destination-wildcard* | **host** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Extended MAC access list (700 to 799)

access-list *id* {**deny** | **permit**} {**any** | **host** *source-mac-address*} {**any** | **host** *destination-mac-address*} [*ethernet-type*][**cos** [*out*][**inner** *in*]]

Extended expert access list (2700 to 2899)

access-list *id* {**deny** | **permit**} [**protocol** | [*ethernet-type*][**cos** [*out*][**inner** *in*]]] [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**}][**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

When you select the Ethernet-type field or cos field:

access-list *id* {**deny** | **permit**} {*ethernet-type*| **cos** [*out*][**inner** *in*]} [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

When you select the protocol field:

access-list *id* {deny | permit} **protocol [VID** [*out*][**inne**r *in*]] {**source** *source-wildcard* | host *source* | **any**} {**host** *source-mac-address* | **any** }{destination *destination-wildcard* | **host** *destination* | **any}** **{host** *destination-mac-address* | **any} [precedence** *precedence*] [**tos** *tos*] **[fragment]** [**range** *lower* *upper*] **[time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

access-list *id* {**deny** | **permit**} **icmp** [**VID** [*out*][**inner** *in*]] {**source** *source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

access-list *id* {**deny** | **permit**} **tcp** [**VID** [*out*][**inner** *in*]]{**source** *source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [**operator** port [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

access-list *id* {**deny** | **permit**} **udp**[**VID** [*out*][**inner** *in*]] {**source** *source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [**operator port** [*port*]] {**destination** *destination-wildcard* | **host** *destination* | **any**}{**host** *destination-mac-address* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

List remark

access-list *id* **list-remark** *text*

Parameter Description

Parameter	Description
id	Access list ID. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.
deny	If not matched, access is denied.
permit	If matched, access is permitted.
source	Specify the source IP address (host address or network address).
source-wildcard	It can be discontinuous, for example, 0.255.0.32.
protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
destination	Specify the destination IP address (host address or network address).
destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
fragment	Packet fragment filtering
precedence	Specify the packet priority.
precedence	Packet precedence value (0 to 7)
range	Layer4 port number range of the packet.
lower	Lower limit of the layer4 port number.
upper	Upper limit of the layer4 port number.
time-range	Time range of packet filtering
time-range-name	Time range name of packet filtering

tos	Specify type of service.
tos	ToS value (0 to 15)
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name
operator	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)
port [*port*]	Port number; *range* needs two port numbers, while other operators only need one port number.
host *source-mac-address*	Source physical address
host *destination-mac-address*	Destination physical address
VID *vid*	Match the specified VID.
ethernet-type	Ethernet type
match-all	Match all the bits of the TCP flag.
tcp-flag	Match the TCP flag.
established	Match the RST or ACK bits, not other bits of the TCP flag.
text	Remark information

Defaults None

Command Mode Global configuration mode.

Usage Guide To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs:

The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses.

The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses.

The extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.

The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID.

For the layer-3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence*/**tos** *tos*/**fragments**/**range** *lower upper*/**time-range** *time-range-name*

The TCP Flag includes part or all of the following:

- urg
- ack
- psh
- rst
- syn
- fin

The packet precedence is as below:

- critical

- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service types are as below:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The ICMP message types are as below:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable

- precedence-unreachable
- protocol-unreachable
- redirect
- device-advertisement
- device-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The TCP ports are as follows. A port can be specified by port name and port number:

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- ldp
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp

- whois
- www

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

The Ethernet types are as below:

- aarp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo

- xns-idp

Configuration Examples

1. Example of the standard IP ACL

The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
Ruijie (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
Ruijie(config)#access-list 102 permit tcp any any eq domain log
Ruijie(config)#access-list 102 permit udp any any eq domain log
Ruijie(config)#access-list 102 permit icmp any any echo log
Ruijie(config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below:

```
Ruijie(config)#access-list 702 deny host 00d0f8000c0c any aarp
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Ruijie(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
Ruijie(config)# access-list 2702 permit any any any any
Ruijie(config)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

Related Commands

Command	Description
show access-lists	Show all the ACLs.
mac access-group	Apply the extended MAC ACL on the interface.

Platform Description

-

clear counters access-list

Use this command to clear the access list counters.

clear counters access-list [*id* | *name*]

Parameter

Parameter	Description

Description

id	ACL ID.
name	ACL name.

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the counters of the specified access list or all access lists.

Configuration Examples

The following example clears the counters of access list 2700:

```
Ruijie #show access-lists 2700
expert access-list extended 2700
   10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any  (88 matches)
   20 deny tcp any any eq login any any (33455 matches)
   30 permit tcp any any host 192.168.6.9 any (10 matches)

Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# clear counters access-list 2700
Ruijie(config)# end
Ruijie #show access-lists 2700
expert access-list extended 2700
   10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
   20 deny tcp any any eq login any any
   30 permit tcp any any host 192.168.6.9 any
```

Related Commands

Command	Description
expert access-list	It indicates the definition of the expert ACL.
deny	The definition denies semantic ACL entries.
permit	The definition permits semantic ACL entries.

Platform Description

deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

Standard IP ACL

[*sn*] **deny** {*source source-wildcard* | **host** *source* | **any| interface** *idx* }[**time-range** *tm-range-name*] [**log**]

Extended IP ACL

[*sn*] **deny protocol source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Extended IP ACLs of some important protocols:

Internet Control Message Prot (ICMP)

[*sn*] **deny icmp** {**source** *source-wildcard* | **host** *source* | **any**} {**destination** *destination-wildcard* | **host** *destination* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] deny udp {*source source –wildcard* | **host** *source* | **any**} [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

[*sn*] deny udp {*source source –wildcard* | **host** *source* | **any**} [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended MAC ACL

[*sn*] **deny** {**any** | **host** *source-mac-address*}{**any** | **host** *destination-mac-address*} [*ethernet-type*][**cos** [*out*] [**inner** *in*]]

Extended expert ACL

[*sn*] **deny**[**protocol** | [*ethernet-type*][**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

When you select the ethernet-type field or cos field:

[*sn*] **deny** {[*ethernet-type*}[**cos** [*out*] [**inner** *in*]]} [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

When you select the protocol field:

[*sn*] **deny protocol** [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destinationdestination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols

Internet Control Message Protocol (ICMP)

[*sn*] **deny icmp** [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any**} {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **deny tcp** [[**VID** [*out*][**inner** *in*]]]{*source source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*]

[**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **deny udp** [[**VID** [*out*][**inner** *in*]]]{*source source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**}{**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **deny arp** {**vid** *vlan-id*}[*source-mac-address source-wildcard* **|host** *source-mac-address* | **any**] [**host** *destination –mac-address* | **any**] {*sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any**} {*sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any**} {*target-ip target-ip–wildcard* | **host** *target-ip* | **any**}

Extended IPv6 ACL

[*sn*] **deny protocol**{*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* } {*destination-ipv6-prefix / prefix-length* | **any**| *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended ipv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*]**deny icmp** {*source-ipv6-prefix / prefix-length* | *any source-ipv6-address* | **host**} {*destination-ipv6-prefix / prefix-length*| **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **deny tcp** {*source-ipv6-prefix / prefix-length* | **host***source-ipv6-address* | **any**}[*operator* **port**[*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[sn] **deny udp** {*source-ipv6-prefix/prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*]] {*destination-ipv6-prefix /prefix-length* | **host** *destination-ipv6-address* | **any**}[*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Parameter Description

Parameter	Description
sn	ACL entry sequence number
source-ipv6-prefix	Source IPv6 network address or network type
destination-ipv6-prefix	Destination IPv6 network address or network type
prefix-length	Prefix mask length
source-ipv6-address	Source IPv6 address
destination-ipv6-address	Destination IPv6 address
dscp	Differential Service Code Point
dscp	Code value, within the range of 0 to 63
flow-label	Flow label
flow-label	Flow label value, within the range of 0 to 1,048,575.
protocol	For the IPv6, the field can be ipv6 | icmp | tcp | udp and number in the

	range 0 to 255
time-range	Time range of the packet filtering
time-range-name	Time range name of the packet filtering

Defaults No entry

Command mode ACL configuration mode.

Usage Guide Use this command to configure the filtering entry of ACLs in ACL configuration mode.

Configuration Examples The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Ruijie(config)#expert access-list extended 2702
Ruijie(config-exp-nacl)#deny tcp  host
192.168.4.12 host 0013.0049.8272 any any
Ruijie(config-exp-nacl)#permit any any any any
Ruijie(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
Ruijie(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)# ip access-list extended ip-ext-acl
Ruijie(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ip access-group ip-ext-acl in
Ruijie(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#mac access-list extended mac1
Ruijie(config-mac-nacl)#deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ip access-list standard 34
Ruijie(config-ext-nacl)# deny host 192.168.4.12
Ruijie(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
Ruijie(config-ext-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ip access-group 34 in
```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#11 deny ipv6 host 192.168.4.12 any
Ruijie(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ipv6 traffic-filter v6-acl in
```

Related Commands

Command	Description
show access-lists	Show all the ACLs.
ipv6 traffic-filter	Apply the extended ipv6 ACL on the interface.
ip access-group	Apply the IP ACL on the interface.
mac access-group	Apply the extended MAC ACL on the interface.
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.
permit	Permit the access.

Platform Description

-

expert access-group

Use this command to apply the specified expert ACL on the specified interface. Use the **no** form of the command to remove the application.

expert access-group {*id*|*name*} {**in**|**out**}

no expert access-group {*id*|*name*} {**in**|**out**}

Parameter Description

Parameter	Description
id	ID of the expert ACL (2700 to 2899)
name	Name of the expert ACL
in	Filter the inputting packets of the interface
out	Filter the outputting packets of the interface

Defaults

No Expert ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage Guide

This command is used to apply the specified ACL on the interface to control the input and output data streams on the interface. Use the **show access-group** command to show the setting.

Configuration Examples

The following example shows how to apply the **access-list** ***accept***_00d0f8xxxxxx only to Gigabit interface 0/1:

```
Ruijie(config)# interface GigaEthernet 0/1
Ruijie(config-if)# expert access-group
accept_00d0f8xxxxxx_only in
```

Related Commands

Command	Description
show access-group	Show the ACL configuration.

Platform Description

N/A

expert access-list

Use this command to create an extended expert ACL. Use the **no** form of the command to remove the ACL.

expert access-list extended {*id* | *name*}

no expert access-list extended {*id* | *name*}

Parameter Description

Parameter	Description
id	ID of the extended expert ACL (2700 to 2899)
name	Name of the extended expert ACL

Defaults

No Expert ACL

Command mode

Global configuration mode.

Usage Guide

Use **show access-lists** to display the ACL configurations**.**

Configuration Examples

Create an extended expert ACL:

```
Ruijie(config)# expert access-list extended exp-acl
Ruijie(config-exp-nacl)#  show  access-lists  expert  access-list  extended
exp-acl
Ruijie(config-exp-nacl)#
```

Create an extended expert ACL:

```
Ruijie(config)# expert access-list extended 2704
Ruijie(config-exp-nacl)# show access-lists  access-list extended 2704
Ruijie(config-exp-nacl)#
```

Related Commands

Command	Description
show access-lists	Show the extended expert ACLs

Platform Description

N/A

expert access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

expert access-list new-fragment-mode { *id* **|** *name* }

no expert access-list new-fragment-mode { *id* **|** *name* }

Parameter Description

Parameter	Description
id	It indicates the serial number of the expert ACL, which ranges from 2700 to 2899.
name	It indicates the name of the ACL.

Defaults

Use the default matching mode of fragmentation packets. By default, if the ACL rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the ACL rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

Command mode

Global configuration mode

Usage Guide

Use this command to switch and control the matching mode of ACL rules to fragmentation packets.

Use the **show running** command to show the setting.

Configuration Examples

The following example switches the matching mode of fragmentation packets for the ACL No. 2700 from the default mode to a new matching mode:

```
Ruijie(config)#expert access-list new-fragment-mode 2700
```

Related Commands

Command	Description
-	-

Platform Description

N/A

expert access-list counter

Use this command to enable the packet matching counter for all ACEs under the expert ACL. Use the **no** form of this command to disable the function.

expert access-list counter { *id* | *name* }

no expert access-list counter { *id* | *name* }

Parameter Description

Parameter	Description
id	ID of the expert ACL, which ranges from 2700 to 2899.
name	Name of the ACL.

Defaults

The packet matching counter of the expert ACL is disabled.

Command mode

Global configuration mode

Usage Guide

Use the **show expert access-lists** command to show the configuration of this command.

Configuration Examples

Example 1 enables the packet matching counter of the extended expert ACL:

```
Ruijie(config)# expert access-list counter exp-acl
Ruijie(config)# show access-lists
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (16 matches)
 20 deny tcp any any eq login any any (78 matches)
```

Example 2 disables the packet matching counter of the extended expert ACL:

```
Ruijie(config)#no expert access-list counter exp-acl
Ruijie(config)# show access-lists
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
 20 deny tcp any any eq login any any
```

Related Commands

Command	Description
show access-lists	Show the extended expert ACL.

Platform Description

N/A

global ip access-group

The ACL is applied on all interfaces by default. The **no** form of this command cancels the application. Use the **global ip access-group** command to restore the application.

global ip access-group

no global ip access-group

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The ACL is applied on all interfaces.

Command mode

Interface configuration mode

Usage Guide

The **no** form of this command is used to cancel the application of the ACL on a specific interface.

Configuration Examples

The following example cancels the application of the ACL on fastEthernet0/0:

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if)#no global ip access-group
```

Related Commands

Command	Description
ip access-group	Apply the ACL globally

Platform Description

N/A

ip access-group

Use this command to apply a specific ACL to an interface. The **no** form of this command cancels the application.

ip access-group {*id* | *name*} {**in** | **out**}

no ip access-group { *id* | *name*} {**in** | **out**}

Parameter Description

Parameter	Description
id	ID of the IP ACL (1 to 199, 1300 to 2699)
name	Name of the IP ACL
in	Filter the incoming packets of the interface.
out	Filter the outgoing packets of the interface.

Defaults

No ACL is applied on the interface.

Command mode

Interface configuration mode/global configuration mode.

Usage Guide

Use the **ip access-group** command to apply the specified ACL to the interface, when the firewall is enabled.

Configuration Examples

The following example applies the ACL 120 on the fastEthernet0/0 to filter the incoming packets:

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if)# ip access-group 120 in
```

Related Commands

Command	Description
access-list	Define the ACL.
show access-lists	Show all the ACLs.

Platform Description

-

ip access-list

Use this command to create a standard IP ACL or extended IP ACL. Use the **no** form of the 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 the ACL 1 to 99 and 1300 to 1999 for standard ACL) or 100 to 199 and 2000 to 2699 for extended ACL
name	Name of the ACL

Defaults

None

Command mode

Global configuration mode.

Usage Guide

There are differences between a standard ACL and an extended ACL. The extended ACL is more precise. Refer to **deny** or **permit** in the two modes. Use **show access-lists** to display the ACL configurations**.**

Configuration Examples

Create a standard ACL:

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
Ruijieconfig-std-nacl)#
```

Create an extended ACL:

```
Ruijie(config)# ip access-list extended 123
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 123
Ruijie(config-ext-nacl)#
```

Related Commands

Command	Description
show access-lists	Show the ACLs.

Platform Description

-

ip access-list log-update interval

Use this command to configure the interval at which the packet matching log of the IPv4 ACL is updated. Use the **no** form of this command to restore the default value.

ip access-list log-update interval *time*

no ip access-list log-update interval

Parameter Description

Parameter	Description
time	For the ACL rule with the log output option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is five minutes, indicating that the ACL matching log of a specified flow is output every five minutes. 0 indicates that no ACL logging is output.

Defaults

The default interval at which the packet matching log of IPv4 ACL is updated is five minutes.

Command mode

Global configuration mode

Usage Guide

This command is used to configure the interval at which the packet matching log of IPv4 ACL is updated.

Configuration Examples

The following example configures the minimum interval for packet matching log updating of IPv4 ACL to 10 minutes:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip access-list log-update interval 10
```

Related Commands

Command	Description
ip access-list	It indicates the definition of the IPv4 ACL.
deny	The definition denies semantic ACL entries.
permit	The definition permits semantic ACL entries.

Platform Description

ip access-list counter

Use this command to enable the packet matching counter for all ACEs under the standard and extended IP ACL. Use the **no** form of this command to disable the function.

ip access-list counter { *id* | *name* }

no ip access-list counter { *id* | *name* }

Parameter Description

Parameter	Description
id	Number of the IP ACL. The standard IP ACL number ranges from 1 to 99, and from 1300 to 1999, and the extended IP ACL ranges from 100 to 199, and from 2000 to 2699.
name	Name of the IP ACL.

Defaults

No ACL is configured.

Command mode

Global configuration mode

Usage Guide

Use the **show access-lists** command to show the setting of ACL.

Configuration Examples

Example 1 enables the packet counter for the standard ACL:

```
Ruijie(config)# ip access-list counter std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255 (999 matches)
 20 deny host 5.5.5.5 time-range tm (2000 matches)
```

Example 2 disables the packet counter for the standard ACL:

```
Ruijie(config)#no ip access-list counter std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255
 20 deny host 5.5.5.5 time-range tm
```

Related Commands

Command	Description
show access-lists	Show IP ACLs.

Platform Description

ip access-list new-fragment-mode

Use this command to switch the matching mode of fragmentation packets of extended IP ACL. Use the **no** form of this command to restore the default matching mode of fragmentation packets.

ip access-list new-fragment-mode { *id* **|** *name* }

no ip access-list new-fragment-mode { *id* **|** *name* }

Parameter Description

Parameter	Description
id	It indicates the number of the extended IP ACL, which ranges from 100 to 199, and from 2000 to 2699.
name	Name of the extended IP ACL

Defaults

Use the default matching mode of fragmentation packets. By default, if the ACL rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the ACL rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.

Command mode

Global configuration mode

Usage Guide

This command is used to switch and control the fragmentation packet matching mode of ACL rules. Use the **show running** command to show the setting.

Configuration Examples

The following example switches the fragmentation packet matching mode of the ACL No.100 from the default mode to a new mode:

```
Ruijie(config)#ip access-list new-fragment-mode 100
```

Related

Command	Description

Commands

-	-

Platform Description

ip access-list resequence

Use this command to rearrange entries of an IP ACL and enter the 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	It indicates the number of the ACL.
name	It indicates the name of the ACL.
start-sn	It indicates the start value of the sequence number.
inc-sn	It indicates the increment of the sequence number.

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use the **show access-lists** command to show 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	It is used to show the ACL.

Platform Description -

ipv6 access-list

Use this command to create an extended IPv6 ACL and enter the 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	It indicates the name of the ACL.

Defaults -

Command mode Global configuration mode

Usage Guide Use the **show access-lists** command to show 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 access-lists	It is used to show the extended IPv6 ACL.

Platform Description -

ipv6 access-list log-update interval

Use this command to configure the interval at which the packet matching log of the IPv6 ACL is updated. Use the **no** form of this command to restore the default value.

ipv6 access-list log-update interval *time*

no ipv6 access-list log-update interval

Parameter Description

Parameter	Description

time	For the ACL rule with the logging output option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is five minutes, indicating that the ACL matching log of a specific flow is output every five minutes. 0 indicates that no ACL logging is output.

Defaults The interval at which the packet matching log of IPv6 ACL is updated is five minutes.

Command mode Global configuration mode

Usage Guide This command is used to configure the interval at which the packet matching log of the IPv6 ACL is updated.

Configuration Examples The following example configures the minimum interval for packet matching log updating of the IPv6 ACL to 10 minutes:

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 access-list log-update interval 9
```

Related Commands

Command	Description
ipv6 access-list	It indicates the definition of the IPv6 ACL.
deny	The definition denies semantic ACL entries.
permit	The definition permits semantic ACL entries.

Platform Description

ipv6 access-list counter

Use this command to enable the packet matching counter for all ACEs under the extended IPv6 ACL. Use the **no** form of this command to disable the function.

ipv6 access-list counter *name*

no ipv6 access-list counter *name*

Parameter Description

Parameter	Description
name	It indicates the name of the ACL.

Defaults -

Command mode Global configuration mode

Usage Guide

Use the **show access-lists** command to show the configuration of this command.

Configuration Examples

Example 1 enables the packet matching function of the extended IPv6 ACL:

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any (7 matches)
 20 deny tcp any any (7 matches)
```

Example 2 disables the packet matching function of the extended IPv6 ACL:

```
Ruijie(config)#no ipv6 access-list v6-acl counter
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
 10 permit icmp any any
20 deny tcp any any
```

Related Commands

Command	Description
show access-lists	It is used to show extended IPv6 ACL.

Platform Description

ipv6 traffic-filter

Use this command to apply the specified IPV6 ACL on the specified interface. Use the **no** form of the command to remove the application.

ipv6 traffic-filter *name* {**in** | **out**}

no ipv6 traffic-filter *name* {**in** | **out**}

Parameter Description

Parameter	Description
name	Name of IPv6 ACL
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface

Defaults

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage Guide

Apply the specified IPV6 ACL on the specified interface to control the interface traffic. You can show the configuration by command **show ipv6 traffic-filter.**

Configuration Examples

The following example shows how to apply the **access-list v6-acl** to 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	Show the ACL configurations.

Platform Description

-

list-remark text

Use this command to add remarks for the specified ACL. The **no** form deletes the remarks.

list-remark *text*

Parameter Description

Parameter	Description
text	Remark information

Defaults

-

Command mode

ACL configuration mode

Usage Guide

Add remarks for the specified ACL.

Note: The remarks include 100 characters at most and two same remarks are not allowed in one ACL.

When an ACE is deleted, the remarks between this ACE and the preceding one are deleted.

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	Show the ACLs.

ip access-list	Define the IP ACL.

Platform Description

-

mac access-group

Use this command to apply the specified MAC ACL on the specified interface. Use the **no** form of the command to remove the application.

mac access-group {*id* | *name*}{**in** | **out**}

no mac access-group {*id* | *name*} {**in** | **out**}

Parameter Description

Parameter	**Description**
id	ID of the MAC ACL (700 to 799)
name	Name of the MAC ACL
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface

Defaults

No ACL is applied on the interface.

Command mode

Interface configuration mode.

Usage Guide

You can use the **show running-config** command to show the configuration result.

Configuration Examples

The following example shows how to apply the **access-list accept**_00d0f8xxxxxx only to Gigabit interface 1:

```
Ruijie(config)#interface GigaEthernet 1/1
Ruijie(config-if)#mac access-group
accept__00d0f8xxxxxx_only in
```

Related Commands

Command	**Description**
show access-group	Show the ACL configuration.

Platform Description

mac access-list

Use this command to create an extended MAC ACL. Use the **no** form of the command to remove the ACL.

mac access-list extended {*id* | *name*}

no mac access-list extended {*id* | *name*}

Parameter Description

Parameter	Description
id	ID of the extended MAC ACL (700 to 799)
name	Name of the extended MAC ACL

Defaults None

Command mode Global configuration mode.

Usage Guide Use the **show access-lists** command to display the ACL configurations**.**

Configuration Examples

Create an extended MAC ACL**:**

```
Ruijie(config)# mac access-list extended mac-acl
Ruijie(config-mac-nacl)# show access-lists mac access-list extended mac-acl
```

Create an extended ACL:

```
Ruijie(config)# mac access-list extended 704
Ruijie(config-mac-nacl)# show access-lists mac access-list extended 704
```

Related Commands

Command	Description
show access-lists	Show the ACLs

Platform Description

mac access-list counter

Use this command to enable the packet matching counter for all ACEs under the extended MAC ACL. Use the **no** form of this command to disable the function.

mac access-list counter { *id* | *name* }

no mac access-list counter { *id* | *name* }

Parameter Description

Parameter	Description
id	It indicates the number of the MAC ACL, which ranges from 700 to 799.
name	It indicates the name of the MAC ACL.

Defaults No MAC ACL is configured.

Command mode Global configuration mode

Usage Guide

Use the **show access-lists** command to show the configuration of this command.

Configuration Examples

Example 1 enables the ACE packet matching counter of the extended MAC ACL:

```
Ruijie(config)# mac access-list extended mac-acl
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac-acl
 10 permit host 0023.56ac.8965 any (170 matches)
 20 deny any any etype-any cos 6 (239 matches)
```

Example 2 disables the ACE packet matching counter of the extended MAC ACL:

```
Ruijie(config)#no mac access-list extended mac-acl counter
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac-acl
10 permit host 0023.56ac.8965 any
20 deny any any etype-any cos 6
```

Related Commands

Command	Description
show access-lists	It is used to show extended MAC ACL.

Platform Description

no sn

Use this command to delete an entry of the ACL.

no *sn*

Parameter Description

Parameter	Description
sn	Sequence number of the ACL entry

Defaults

-

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	Show all the ACLs.
ip access-list	Define the IP ACL.
ipv6 access-list	Define the extended IPV6 ACL.
deny	Define the deny rule.
permit	Define the permit rule.

Platform Description

-

permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

Standard IP ACL

[*sn*] **permit** {*source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*] [**log**]

Extended IP ACL

[*sn*] **permit protocol** *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** {*source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** { *source source-wildcard* | **host** *source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** {*source source -wildcard*|**host** *source* |**any**} [*operator* **port** [*port*]] {*destination destination-wildcard* |**host** *destination* | **any**} [**operator port** [*port*]] [**precedence** *precedence*] [**tos**

tos] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended MAC ACL

[*sn*] **permit** {**any** | **host** *source-mac-address*} {**any** | **host** *destination-mac-address*} [*ethernet-type*][**cos** [*out*] [**inner** *in*]]

Extended expert ACL

[*sn*] **permit** [**protocol** | [*ethernet-type*][**cos** [*out*] [**inner** *in*]]] [**VID** [*out][***inner** *in]*] {*source source-wildcard* | **host** *source* | **any**} {**host** *source*-mac-*address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*][**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

When you select the Ethernet-type field or cos field:

[*sn*] **permit** {*ethernet-type*| **cos** [*out*] [**inner** *in*]} [**VID** [*out*][**inner** *in*]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**time-range** *time-range-name*]

When you select the protocol field:

[*sn*] **permit protocol** [**VID** [*out][***inner** *in*]] {*source source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** [**VID** [*out*][**inner** *in*]] {*source source-wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**}[*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** [**VID** [*out*][**inner** *in*]]{*source source-wildcard* | **host** *Source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** [**VID** [*out*][**inner** *in*]]{*source source –wildcard* | **host** *source* | **any**} {**host** *source-mac-address* | **any** } [*operator* **port** [*port*]] {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [*operator* **port** [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **permit arp** {**vid** *vlan-id***}** [**host** *source-mac-address* | **any**] [**host** *destination –mac-address* | **any**] {*sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any**} {*sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any**} {*target-ip target-ip–wildcard* | **host** *target-ip* | **any**}

Extended IPv6 ACL

[*sn*] **permit protocol** {*source-ipv6-prefix* / *prefix-length* | **any** | **host** *source-ipv6-address*} {*destination-ipv6-prefix* / *prefix-length* | **any**| *hostdestination-ipv6-address*} [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended IPv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** {*source-ipv6-prefix* / *prefix-length* | **any** *source-ipv6-address* | **host**}

{*destination-ipv6-prefix* / *prefix-length*| **host** *destination-ipv6-address* | **any**} [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**dscp** *dscp*] [**flow-label** *flow-label*][**fragment**] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** {*source-ipv6-prefix* / *prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*]] {*destination-ipv6-prefix* / *prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**match-all** *tcp-flag* | **established**]

User Datagram Protocol (UDP)

[*sn*] **permit udp** {*source-ipv6-prefix* / *prefix-length* | **host** *source-ipv6-address* | **any**} [*operator* **port** [*port*]] {*destination-ipv6-prefix* / *prefix-length* | **host** *destination-ipv6-address* | **any**} [*operator* **port** [*port*]] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

Parameter Description

Parameter	Description
-	-

Defaults

None

Command mode

ACL configuration mode.

Usage Guide

Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.

Configuration Examples

The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Ruijie(config)#expert access-list extended exp-acl
Ruijie(config-exp-nacl)#permit tcp  host  192.168.4.12 host 0013.0049.8272
any any
Ruijie(config-exp-nacl)#deny any any any any
Ruijie(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
Ruijie(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
```

```
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ip access-group 102 in
Ruijie(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#mac access-list extended 702
Ruijie(config-mac-nacl)#permit host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
Ruijie(config-mac-nacl)#exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ip access-list standard std-acl
Ruijie(config-std-nacl)#permit host 192.168.4.12
Ruijie(config-std-nacl)#show access-lists
ip access-list standard std-acl
  10 permit host 192.168.4.12
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
Ruijie(config)#ipv6 access-list extended v6-acl
Ruijie(config-ipv6-nacl)#11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
Ruijie(config-ipv6-nacl)# exit
Ruijie(config)#interface gigabitethernet 1/1
Ruijie(config-if)#ipv6 traffic-filter v6-acl in
```

Related Commands

Command	Description
show access-lists	Show all the ACLs.
ipv6 traffic-filter	Apply the extended ipv6 ACL on the interface.
ip access-group	Apply the IP ACL on the interface.
mac access-group	Apply the extended MAC ACL on the interface.
ip access-list	Define the IP ACL.

mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.
deny	Deny the access.

Platform Description

-

remark

Use this command to add remarks for the specified ACE in the ACL. The **no** form deletes the remarks.

remark *text*

Parameter Description

Parameter	Description
text	Remark information

Defaults

-

Command mode

ACL configuration mode.

Usage Guide

Use this command to add remarks for the specified ACE. It is worth mentioning that up to 100 characters are allowed to be contained in the remark. 2 same ACE remarks in 1 ACL is not allowed.

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	Show the ACLs.
ip access-list	Define the IP ACL.

Platform Description

security access-group

Use this command to configure the secure interface channel.

security access-group {*id*|*name*}

no security access-group

Parameter Description

Parameter	Description
id	It indicates the ID of the ACL.
name	It indicates the name of the ACL.

Defaults -

Command mode Interface configuration mode

Usage Guide This command is used to configure the secure interface channel.

Configuration Examples

```
Ruijie(config-if)#security access-group 1
```

Related Commands

Command	Description
show running	It shows the current configuration information.

Platform Description

security global access-group

Use this command to configure the global security channel.

security global access-group { *id* | *name* **}**

no security global access-group

Parameter Description

Parameter	Description
id	ACL ID
name	ACL name

Defaults -

Command mode Global configuration mode

Usage Guide Use this command to configure the global security channel.

Configuration Examples

```
Ruijie# security global access-group 1
```

Related Commands

Command	Description
show running	Show configuration of current system.

Platform Description

security uplink enable

Use this command to configure the uplink port of the security channel on the interface.

security uplink enable

no security uplink enable

Parameter Description

Parameter	Description
-	-

Defaults -

Command mode Interface configuration mode.

Usage Guide Use this command to configure the uplink port of the security channel on the interface.

Configuration Examples

```
Ruijie(config-if)#security uplink enable
```

Related Commands

Command	Description
show running	Show configuration of current system.

Platform Description

show access-group

Use this command to show the ACL configured on the interface.

show access-group [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults -

Command mode Privileged EXEC mode

Usage Guide Show the ACL configured of the interface. If no interface is specified, the associated ACLs of all the interfaces will be shown.

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	Apply the IP ACL to the interface.
mac access-group	Apply the mac ACL to the interface.
expert access-group	Apply the expert ACL to the interface.
ipv6 traffic-filter	Apply the IPv6 ACL to the interface.

Platform Description -

show access-lists

Use this command to show all ACLs or the specified ACL.

show access-lists [*id* | *name*]

Parameter Description

Parameter	Description
id	ID of the IP ACL
name	Name of the IP ACL

Defaults -

Command mode

Privileged EXEC mode

Usage Guide

Use this command to show the specified ACL. If no ID or name is specified, all the ACLs will be shown.

Configuration Examples

```
Ruijie# show access-lists n_acl
ip access-list standard n_acl
Ruijie# show access-lists 102
ip access-list extended 102
Ruijie# show access-lists
ip access-list standard n_acl
ip access-list extended 101
permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
permit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

Related Commands

Command	Description
ip access-list	Define the IP ACL.
mac access-list	Define the extended MAC ACL.
expert access-list	Define the extended expert ACL.
ipv6 access-list	Define the extended IPv6 ACL.

Platform Description

-

show expert access-group

Use this command to show the configured expert ACL of the interface.

show expert access-group [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults

-

Command mode

Privileged EXEC mode

Usage Guide

Show the expert ACL configured on the interface. If no interface is specified, the associated expert ACLs of all the interfaces will be shown.

Configuration Examples

```
Ruijie# show expert access-group interface gigabitethernet 0/2
expert access-group ee in
Applied On interface GigabitEthernet 0/2.
```

Related Commands

Command	Description
expert access-list	Define the extended expert ACL.

Platform Description

-

show ip access-group

Use this command to show the configured expert ACL of the interface.

show ip access-group[**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults

-

Command mode

Privileged EXEC mode

Usage Guide

Show the IP ACL configured of the interface. If no interface is specified, the associated IP ACLs of all the interfaces will be shown.

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	Define the IP ACL.

Platform Description

-

show ipv6 traffic-filter

Use this command to show the configured IPv6 ACL of the interface.

show ipv6 traffic-filter [**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults -

Command mode Privileged EXEC mode

Usage Guide Show the IPv6 ACL associated with the interface. If no interface is specified, the associated IPv6 ACLs of all the interfaces will be shown.

Configuration Examples

```
Ruijie# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/4.
```

Related Commands

Command	Description
ipv6 access-list	Define the type of IPv6 ACL.

Platform Description -

show mac access-group

Use this command to show the configured MAC ACL of the interface.

show mac access-group[**interface** *interface*]

Parameter Description

Parameter	Description
interface	Interface ID

Defaults -

Command mode Privileged EXEC mode

Usage Guide Show the MAC ACL associated with the interface. If no interface is specified, the associated MAC ACLs of all associated interfaces will be shown.

Configuration Examples

```
Ruijie# show mac access-group interface gigabitethernet 0/3
mac access-group mm in
Applied On interface GigabitEthernet 0/3.
```

Related Commands

Command	Description
mac access-list	Define the extended MAC ACL.

Platform Description

-

QoS Configuration Commands

Default Configuration

Before configuring QoS, you must have a full knowledge of these items related to QoS:

1) One interface can only be associated with one policy map at most.
2) One policy map may own multiple class maps
3) One class map can be associated with only one ACL, and all the ACEs of this ACL must have the same filter domain template.
4) The number of ACEs associated with an interface complies with the restriction given in "*Configuring Security ACLs*".

The QoS function is disabled by default. Namely the device processes all the packets in the same way. But if you associate a policy map with an interface and the trust mode on one interface, the QoS of this interface is enabled automatically. To disable the QoS function of the interface, simply resolve the policy map setting of the interface and set the information mode of the interface to Off. Below is the default QoS configuration:

Default Settings	**Default CoS value**	0
	Queue Number	8
	Queue Scheduling	WRR
	Queue Weight	1:1:1:1:1:1:1:1
	WRR Weight Range	1:254
	DRR Weight Range	1:254
	Trust mode	No Trust

Default Cos to queue mapping table:

	CoS value	Queue
Cos to Queue	0	1
	1	2
	2	3
	3	4
	4	5
	5	6
	6	7
	7	8

Default CoS to DSCP mapping table

	CoS value	DSCP value
CoS to DSCP	0	0
	1	8
	2	16
	3	24
	4	32

5	40
6	48
7	56

Default IP Precedence to DSCP mapping table.

IP-Precedence to DSCP

IP-Precedence	DSCP
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Default DSCP to Cos mapping table.

DSCP to CoS

DSCP value	CoS value
0	0
8	1
16	2
24	3
32	4
40	5
48	6
56	7

class maps

Use the following command to create an ACL:

ip access-list { **extended** | **standard** } { *acl-id* | *acl-name* }

Or **mac access-list extended** { acl-id | acl-name }

Or **expert access-list extended** { acl-id | acl-name }

Or **ipv6 access-list extended** *acl-name*

Or **access-list** *acl-id* series commands (refer to the related ACL chapters)

Use the following command to create a class map and enter the class map configuration mode:

no class-map *class-map-name*

Use the following command to create the matching standard of class map:

[**no**] **match access-group** *acl-name* **|** *acl-id*

[**no**] **match ip dscp** *dscp-value1* [*dscp-value2* [*dscp-valueN*]]

[**no**] **match ip precedence** *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]

Parameter Description

Parameter	Description
acl-name	Name of the created ACL

acl-id	ID of the created ACL
class-map-name	Name of the class map to be created
dscp-valueN	IP dscp value to be matched..
ip-pre-valueN	IP precedence value to be matched.
no class-map *class-map-name*	Delete the existing class map.
no match access-group *acl-name* | *acl-id*	Delete the match.
no match ip dscp *dscp-value1* [*dscp-value2* [*dscp-valueN*]]	Delete the matched ip dscp value.
no match ip precedence *ip-pre-value1* [*ip-pre-value2* [*ip-pre-valueN*]]	Delete the matched ip precedence value.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples

Create an extended MAC ACL named **me**.

```
Ruijie(config)# mac access-list extended me
```

Set ACL rules.

```
Ruijie(config-ext-macl)# permit host 1111.2222.3333 any
```

Exit the ACL setting.

```
Ruijie(config-ext-macl)# exit
```

Create a class map named **cm.**

```
Ruijie(config)# class-map cm
```

Associate the class map with the ACL.

```
Ruijie(config-cmap)# match access-group me
```

Exit the class map setting.

```
Ruijie(config-cmap)# exit
```

Create the class-map named cm-dscp and match the DSCP 8,16,24 and exit the setting.

```
Ruijie(config)# class-map cm-dscp
Ruijie(config-cmap)# match ip dscp 8 16 24
Ruijie(config-cmap)# exit
```

Related Commands

Command	Description
show map access-lists	N/A
show ip access-lists	N/A
show class-map	N/A

Platform Description

N/A

drr-queue bandwidth

Use this command to set the queue weight in the DRR scheduling mode. Use the **no** form of the command to restore it to the default.

drr-queue bandwidth *weight1...weight8*

no drr-queue bandwidth

Parameter Description

Parameter	Description
weight1...weight8	Queue weight. For the value range, see **Default Configuration**.
no	Restore the default value.

Defaults

See **Default Configuration**.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# drr-queue bandwidth 1 2 3 4 5 6 7 8
```

Related Commands

Command	Description
show mls qos queuing	N/A

Platform Description

N/A

interface rate-limit

Use this command to set the rate limit on the port.

rate-limit { input | output } *bps burst-size*

no rate-limit

Parameter Description

Parameter	Description
input	Input rate limit
output	Output rate limit
bps	Limited bandwidth per second
burst-size	The dscp-list range varies with products
no	Restore it to the default value.

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# rate-limit input 1000000 4096
```

Related Commands

Command	Description
show mls qos interface	N/A

Platform Description N/A

mls qos cos

Use this command to configure the CoS value of an interface. Use the **no** form of this command to restore it to the default.

mls qos cos *default-cos*

no mls qos cos

Parameter Description

Parameter	Description
default-cos	Range: 0 to 7
no	Restore the default value.

Defaults The CoS value is 0.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# mls qos cos 7
```

Related Commands

Command	Description
show mls qos interface *interface-id*	N/A

Platform Description N/A

mls qos map cos-dscp

Use this command to map the CoS value to the DSCP value. Use the **no** form of the command to disable the mapping.

mls qos map cos-dscp *dscp1...dscp8*

no mls qos map cos-dscp

Parameter Description

Parameter	Description
dscp	Specify the DSCP value.
no	Restore the default value.

Defaults

See **Default Configuration**.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# mls qo map cos-dscp 8 10 16 18 24 26 32 34
```

Related Commands

Command	Description
show mls qos maps	Show DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

Platform Description

N/A

mls qos map dscp-cos

Use this command to map the DSCP value to the COS value. Use the **no** form of the command to disable the mapping.

mls qos map dscp-cos *dscp-list to cos*

no mls qos map dscp-cos

Parameter Description

Parameter	Description
dscp-list	DSCP list. Its range varies with products.
cos	COS value, ranging from 0 to 7
no	Restore the default value.

Defaults

See **Default Configuration**.

Command Mode

Global configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

Related Commands

Command	Description
show mls qos maps	Show DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

Platform Description N/A

mls qos map ip-prec-dscp

Use this command to map the IP-precedence to the DSCP value. Use the **no** form of this command to disable the mapping.

mls qos map ip-prec-dscp *dscp1 ... dscp8*

no mls qos map ip-prec-dscp

Parameter Description

Parameter	Description
dscp	Specify the DSCP value.
no	Restore the default value.

Defaults See **Default Configuration**.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34
```

Related Commands

Command	Description
show mls qos maps	Show the DSCP-COS, COS-DSCP and IP-prec-DSCP maps.

Platform Description N/A

mls qos scheduler

Use this command to configure the output queue scheduling algorithm. Use the **no** form of the command to restore the default.

mls qos scheduler [**sp** | **wrr** | **drr**]

no mls qos scheduler

Parameter Description

Parameter	Description
sp	Absolute priority scheduling
wrr	Frame count weighted round-robin scheduling
drr	Frame length weighted round-robin scheduling
no	Restore the default value.

Defaults

The queue scheduling algorithm is **wrr** by default.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# mls qos scheduler sp
```

Related Commands

Command	Description
show mls qos scheduler	N/A

Platform Description

N/A

mls qos trust

Use this command to configure the trust mode on an interface. Use the **no** form of this command to restore the default.

mls qos trust { **cos** | **dscp** | **ip-precedence** }

no mls qos trust

Parameter Description

Parameter	Description
cos	The QoS trust mode of the port is CoS
dscp	The QoS trust mode of the port is DSCP.
ip-precedence	The QoS trust mode of the port is IP-PRE.
no	Restore the default value.

Defaults

N/A

Command Mode

Interface configuration mode.

Usage Guide

N/A

Configuration

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

Examples

```
Ruijie(config-if)# mls qos trust cos
```

Related Commands

Command	Description
show mls qos interface *interface-id*	N/A

Platform Description

N/A

policy maps

Use the following command to create a policy map and enter the policy map configuration mode.

no policy-map *policy-map-name*

Use the following command to create the class map data classification used in the policy map and enter the data classification configuration mode.

class *class-map-name*

Use the following command to set the ip_dscp value of the IP packets, which does not take effect for non-IP packets.

set ip dscp *new-dscp*

no set ip dscp

Use the following command to set the cos value of the packets. With the none-tos configured, the DSCP value of the packets will not be modified.

set cos *new-cos* [**none-tos**]

no set cos

Use the following command to limit the bandwidth and specify the method of handling the excessive part.

police *rate-bps burst-byte* [**exceed-action** { **drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**] }]

no police

Parameter Description

Parameter	Description
policy-map-name	Name of the policy map to be created
no policy-map *policy-map-name*	Delete the existing policy map.
class-map-name	Name of the created class map
no class *class-map-name*	Delete the class map.
new-dscp	New DSCP value, whose range varies with products.
new-cos	New Cos value, in the range of 0 to 7.
rate-bps	The limitation of bandwidth per second, in kbps
burst-byte	The burst traffic limitation, in Kbyte
drop	Drop the packets exceeding the bandwidth.
dscp-value	Overwrite the DSCP value of the packets exceeding the bandwidth, whose range varies with products.
cos-value	Modify the Cos value of the packets of over-bandwidth, in the range of 0 to 7.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Create a policy map and name it as **po**.

```
Ruijie(config)# policy-map po
```

Associate class-map with **cm**.

```
Ruijie(config-pmap)# class cm
```

Set the DSCP value as 10.

```
Ruijie(config-pmap-c)# set ip dscp 10
```

Set the bandwidth as 1M, the burst traffic as 4096k, and the method for handing the excessive part to assign the new DSCP value of 16.

```
Ruijie(config-pmap-c)# police 1000000 4096 exceed-action dscp 16
```

Related Commands

Command	Description
show policy-map	N/A

Platform Description

N/A

priority-queue

Use this command to configure the output queue scheduling algorithm.

priority-queue

no priority-queue

Parameter Description

Parameter	Description
priority-queue	Set the output queue scheduling algorithm as SP.
no priority-queue	Set the output queue scheduling algorithm as WRR.

Defaults

The output queue scheduling algorithm is WRR.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# no priority-queue
```

Related Commands

Command	Description
show mls qos queuing	N/A

Platform Description

N/A

priority-queue cos-map

Use this command to configure the associated CoS value of output queue:

priority-queue cos-map *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]

no priority-queue cos-map

Parameter Description

Parameter	Description
qid	Specified queue id.
cos0 ... cos7	Associated CoS value.
no	Restore the default value.

Defaults

See **Default Configuration**.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)#priority-queue cos-map 1 0 1
```

Related Commands

Command	Description
show mls qos queuing	N/A

Platform Description

N/A

service-policy

Use this command to apply the policy map on the interface or the virtual-group.

service-policy { **input** | **output** } *policy-map-name*

no service-policy { **input** | **output** }

Parameter Description

Parameter	Description
policy-map-name	Name of the created policy map
no	Cancel the application of the policy map on the interface or the virtual-group.

Defaults N/A

Command Mode Interface configuration mode, and virtual-group configuration mode.

Usage Guide N/A

Configuration Examples

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# service-policy input po
Ruijie(config)# virtual-group 3
Ruijie(config-if)# service-policy input po
```

Related Commands

Command	Description
show mls qos interface	N/A

Platform Description N/A

show class-map

Display the content of class map.

show class-map [*class-name*]

Parameter Description

Parameter	Description
class-name	Name of class map.

Defaults Display all class maps.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
class-map	N/A

Platform Description N/A

show mls qos interface

Use this command to display the QoS configuration on the interface.

show mls qos interface [*interface-id*] [**policers**]

Parameter Description

Parameter	Description
interface-id	Interface ID
policers	Show the police associated with the interface

Defaults The QoS information of all ports is shown.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mls qos interface fastEthernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mls qos maps

Use this command to show dscp-cos maps, dscp-cos maps and ip-prec-dscp maps.

show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]

Parameter Description

Parameter	Description
cos-dscp	Show the cos-dscp maps.
dscp-cos	Show the dscp-cos maps.
ip-prec-dscp	Show the ip-prec-dscp maps.

Defaults All QoS maps are shown by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mls qos maps
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mls qos queuing

Use this command to show the QoS queuing information.

show mls qos queuing

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mls qos queuing
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mls qos rate-limit

Use this command to show the rate limit on the interface.

show mls qos rate-limit [**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

```
Ruijie# show mls qos rate-limit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show mls qos scheduler

Use this command to show the information on queue scheduling algorithm.

show mls qos scheduler

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

```
Ruijie# show mls qos scheduler
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show policy-map

Use this command to show the information of the policy map.

show policy-map [*policy-name* [**class** *class-name*]]

Parameter Description

Parameter	Description
policy-name	Name of the policy name
class-name	Name of the class map

Defaults

All policy maps are shown by default.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie# show policy-map
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show virtual-group

Use this command to show the virtual group information.

show virtual-group [*virtual-group-number* | **summary**]

Parameter Description

Parameter	Description
virtual-group-number	Virtual group number, up to 128.
summary	Show the information on all virtual groups.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

```
Ruijie# show virtual-group 1
Ruijie# show virtual-group summary
```

Related Commands

Command	Description
virtual-group	Enable the virtual group.

Platform Description

N/A

wrr-queue bandwidth

Use this command to set the weight ratio for the WRR algorithm. Use the **no** form of the command to restore it to the default.

wrr-queue bandwidth *weight1 ... weightn*

no war-queue bandwidth

Parameter Description

Parameter	Description
weight1...weightn	Weight value specified for the output queues. For the value of *n* and its range, see **Default Configuration**.
no	Restore the default value.

Defaults

weight1: ...: weightn = 1:..:1

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

```
Ruijie(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
```

Related Commands

Command	Description
show mls qos queuing	N/A

Platform Description

See **Default Configuration**.

virtual-group

Use this command to configure a physical port or Aggregate port as the member port of a virtual group. Use the **no** form of this command to remove the member attribute of a virtual group on the port.

virtual-group *virtual-group-number*

no virtual-group *virtual-group-number*

Parameter Description

Parameter	Description
virtual-group-number	Virtual group number, up to 128.

Defaults

By default, the physical port belongs to no virtual-group.

Command Mode

Interface configuration mode.

Usage Guide

The member port joining the virtual group must be physical port or Aggregate Port. The virtual group member ports must be in the same line card (for the chassis-shaped switch) or in the same switch (for the box-shaped switch). If the line card or switch has 48 ports, all member ports shall be distributed on the former 24 ports or the latter 24 ports.

Configuration Examples

The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3:

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if)# virtual-group 3
```

Related Commands

Command	Description
show virtual-group	Show the virtual-group settings.

Platform Description

N/A

Reliability Configuration Commands

1. CFM Configuration Commands
2. REUP Configuration Commands
3. RLDP Configuration Command
4. DLDP Configuration Commands
5. TPP Configuration Commands
6. BFD Configuration Commands
7. RNS&Track Configuration Commands
8. GRTD Configuration Commands
9. SEM Configuration Commands
10. VSU Configuration Commands

CFM Configuration Commands

cfm alarm-priority service-instance mep

Use this command to configure the lowest bug level for MEP to generate the alarm. Use the **no** form of this command to restore the lowest bug level to the default value.

cfm alarm-priority *priority-value* **service-instanc**e *instance-id* [**mep** *mep-id*]

no cfm alarm-priority

Parameter Description

Parameter	Description
instance-id	Service instance id, in the range from 1 to 32767.
no	Restores the lowest bug level to the default value.
mep-id	MEP ID, in the range from 1 to 8191.
priority-value	When the detected bug level is greater or equal to this value, it will send the alarm to the network administrator. This value is in the range from1 to 5. The default value is 2.

Defaults

The default lowest bug level for MEP to generate the alarm is 2.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

```
Ruijie(config)#cfm alarm-priority 3
```

Related Commands

Command	Description
show cfm mep service-instance	Shows the MEP information.

Platform Description

N/A.

cfm cc interval service-instance

Use this command to set interval of transmitting CCM. Use the **no** form of this command to restore the default interval.

cfm cc interval *interval-type* **service-instance** *instance-id*

no cfm cc interval service-instance *instance-id*

Parameter Description

Parameter	Description
interval-type	Configures CCM transmit interval type for the specified service instance. The *interval-type* parameter ranges from 4 to 7.. CCM transmit intervals represented by various interval types are shown below: Interval-type CCM transmit interval 4 1 second 5 10 seconds 6 60 seconds 7 600 seconds
instance-id	Service instance id, in the range from 1 to 32767.
no	Restore the interval type to the default value.

Defaults The default value of interval-type is 4.

Command Mode Global configuration mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie(config)#cfm cc interval 5 service-instance 1
```

Related Commands

Command	Description
cfm cc service-instance enable	Enables the function of transmitting CCM.
show cfm service-instance	Shows the service instance information, including the interval of transmitting the CCM.

Platform Description N/A.

cfm cc service-instance enable

Use this command to enable the CC (Continuity Check) function for the MEP in the service instance. Use the **no** form of this command to disable this function.

cfm cc service-instance *instance-id* [**mep** *mep-id*] **enable**

no cfm cc service-instance *instance-id* [**mep** *mep-id*] **enable**

Parameter Description

Parameter	Description
instance-id	Service instance ID, in the range from 1 to 32767.
mep-id	MEP ID, in the range from 1 to 8191.
no	Disables the function of transmitting CCM on the MEP (Maintenance

	association End Point).

Defaults The CC function is disabled by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie(config)#cfm cc service-instance 1 enable
```

Related Commands

Command	Description
cfm cc interval service-instance	Sets the interval of transmitting CCM.
show cfm mep service-instance	Shows the MEP information, including the transmitting status of CCM.

Platform Description N/A.

cfm linktrace auto-detection size

Use this command to auto-execute the linktrace function when a peer MEP is lost.

cfm linktrace auto-detection [**size** *entries-count*]

no cfm linktrace auto-detection

Parameter Description

Parameter	Description
size *entries-count*	The system saves the reply information of the auto-executed linktrace for entries-count times in total. The range is from 1 t0 100.
no	Disables the linktrace auto-detection function.

Defaults The default entries-count value is 5.

Command Mode Global configuration mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie(config)# cfm linktrace atuto-detection
```

Related Commands

Command	Description

show cfm linktrance auto-detection size	Shows the reply information of the auto-executed linktrace.

Platform Description

N/A.

cfm linktrace service-instance mep ttl

Use this command to execute the linktrace function.

cfm linktrace service-instance *instance-id* **mep** *mep-id* { **remote-mep** *remote-mep-id* | **remote-mac** *mac-address* } [**ttl** *ttl-value*] [**hw-only**]

Parameter Description

Parameter	Description
instance-id	Service instance ID, in the range from 1 to 32767.
mep-id	MEP ID, in the range from 1 to 8191.
remote-mep *remote-mep-id*	Remote MEP ID.
remote-mac *mac-address*	MAC address of the remote MP (including the MEP and MIP).
ttl *ttl-value*	The maximum tops for LTM forwarding, in the range from 1 to 255.
hw-only	Forwards the LTM according to the FDB table only.

Defaults

The ttl-value is 64 and the hw-only option is disabled by default.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

```
Ruijie# cfm linktrace service-instance 1 mep 100 remote-mep 200 ttl 80 hw-only
Ruijie#cfm linktrace service-instance 1 mep 100 remote-mac 00d0.f800.1e2f ttl
30
```

Related Commands

Command	Description
show cfm linktrance-info service-instance	Shows the linktrace information.

Platform Description

N/A.

cfm loopback service-instance mep count

Use this command to execute the loopback function.

cfm loopback service-instance *instance-id* **mep** *mep-id* { **remote-mep** *remote-mep-id* | **remote-mac** *mac-address* } [**count** *count*]

Parameter Description

Parameter	Description
instance-id	Service instance ID, in the range from 1 to 32767.
mep-id	MEP ID, in the range from 1 to 8191.
remote-mep *remote-mep-id*	Remote MEP ID.
remote-mac *mac-address*	MAC address of the remote MP (including the MEP and MIP).
count *count-value*	The number of the LBM to be sent.

Defaults

The default count is 5.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

```
Ruijie# cfm loopback service-instance 1 mep 100 remote-mep 200 count 3
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

cfm ma md

Use this command to create an MA (Maintenance Association). Use the **no** form of this command to delete an MA.

cfm ma *ma-name* **md** *md-name*

no cfm ma *ma-name* **md** *md-name*

Parameter Description

Parameter	Description
no	Deletes a specified MA.
ma-name	Sets the MA name. The range of the name length is from 1 to 43. The summary length of an MA name and an MD name cannot exceed 44.
md-name	Sets the name for the MD where the MA is.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

The summary length of an MA name and an MD name cannot exceed 44, or the MA cannot be created. Besides, an MD shall be created before the creation of an MA.

Configuration Examples

```
Ruijie(config)#cfm ma MA_A_MD_A md MD_A
Ruijie(config)#no cfm ma MA_A_MD_A md MD_A
```

Related Commands

Command	Description
show cfm ma md	Shows the MA information.

Platform Description

N/A.

cfm md level

Use this command to create an MD (Maintenance Domain). Use the **no** form of this command to delete an MD.

cfm md *md-name* **level** *level*

no cfm md *md-name*

Parameter Description

Parameter	Description
md-name	The MD name. The length range is from 1 to 43.
level	The MD level. The level range is from 0 to 7.
no	Deletes an MD.

Defaults

N/A.

Command Mode

Global configuration mode.

Usage Guide

N/A.

Configuration Examples

```
Ruijie(config)#ethernet cfm md MD_A level 5
Ruijie(config)# no ethernet cfm md MD_A
```

Related Commands

Command	Description
show cfm md	Shows the MD information.

Platform Description

N/A.

cfm mep service-instance

Use this command to configure an MEP (Maintenance association End Point). Use the **no** form of this command to delete an MEP.

cfm mep *mep-id* **service-instance** *instance-id* { **inward** | **outward** }

no cfm mep *mep-id* **service-instance** *instance-id*

Parameter Description

Parameter	Description
mep-id	MEP ID, in the range from 1 to 8191.
instance-id	Service instance ID, in the range from 1 to 32767.
inward	Sets the inward MEP.
outward	Sets the outward MEP.
no	Deletes a specified MEP.

Defaults

N/A.

Command Mode

Interface configuration mode.

Usage Guide

N/A.

Configuration Examples

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# cfm mep 100 service-instance 1 inward
```

Related Commands

Command	Description
show cfm mep service-instance	Shows the MEP information.
show cfm mp	Shows the MP information.

Platform Description

N/A.

cfm mep-list service-instance

Use this command to configure an MEP list. Use the **no** form of this command to delete an MEP list.

cfm mep-list *mep-list* **service-instance** *instance-id*

no cfm mep-list *mep-list* **service**-**instance** *instance-id*

Parameter Description

Parameter	Description
mep-list	The MEP list, which could be one MEP or a series of MEPs starting with the low ID and ending with the high one and using the hyphen to link both IDs (such as 10-20). It is based on the privileged view. The

	range of the MEP ID is from 1 to 8191.
instance-id	Service instance ID, in the range from 1 to 32767.
no	Deletes a specified MEP list. The configuration of the local MEPs which are based on this MEP list will be removed.

Defaults N/A.

Command Mode Global configuration mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie(config)# cfm mep-list 1-3 service-instance 1
```

Related Commands

Command	Description
show cfm mep-list service-instance	Shows the MEP list information.

Platform Description N/A.

cfm mip-rule service-instance

Use this command to set the MIP (Maintenance domain Intermediate Point) generation rule. Use the **no** form of this command to delete the MIP generation rule.

cfm mip-rule { **explicit** | **default** } **service-instance** *instance-id*

no cfm mip-rule service-instance *instance-id*

Parameter Description

Parameter	Description
explicit	On condition that there is no MIP in the low-level MD, the MEP in the low-level MD determines whether to create the MIP. If there is a MEP in the low-level MD, then this level will generate a MIP, or else, the MIP will not be created.
default	The MIP generates if there is no MIP in the low-level MD.
instance-id	Service instance ID, in the range from 1 to 32767.
no	Deletes the MIP generation rule and the generated MIPs.

Defaults N/A.

Command Mode Global configuration mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie# cfm mip-rule explicit service-instance 1
```

Related Commands

Command	Description
show cfm mp	Shows the MP information.

Platform Description N/A.

cfm service-instance vlan md ma

Use this command to create a service instance. Use the **no** form of this command to delete a service instance.

cfm service-instance *instance-id* vlan *vlan-id* **md** *md-name* **ma** *ma-name*

no cfm service-instance *instance-id*

Parameter Description

Parameter	Description
instance-id	The service instance ID, in the range from1 to 32767.
md-name	The name of MD where the service instance is.
vlan-id	The VLAN ID of the service instance, in the range from1 to 4094.
ma-name	The MA name.
no	Deletes a service instance.

Defaults N/A.

Command Mode Global configuration mode.

Usage Guide The MA must be created before the creation of the service instance, or the service instance cannot be created.

Configuration Examples

```
Ruijie(config)#cfm service-instance 10 vlan 1 md MD_A ma MA_A_MD_A
Ruijie(config)#no cfm service-instance 10
```

Related Commands

Command	Description
show cfm service-instance	Shows the service instance information.

Platform Description N/A.

show cfm linktrace-info auto-detection size

Use this command to show the auto-detected linktrace information.

show cfm linktrace-info auto-detection [**size** *entries_count*]

Parameter Description

Parameter	Description
entries_count	Entry count, in the range from 1 to 100.

Defaults All auto-detected linktrace information is shown by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

#Show all the auto-detected linktrace information.

```
Ruijie# show cfm linktrace-info auto-detection
```

#Show the linktrace information auto-detected for 10 times.

```
Ruijie# show cfm linktrace-info auto-detection size 10
```

Related Commands

Command	Description
cfm linktrace auto-detection size	Sets the linktrace auto-detection function.

Platform Description N/A.

show cfm linktrace-info service-instance mep

Use this command to show the linktrace information.

show cfm linktrace-info [**service-instance** *instance-id* [**mep** *mep-id*]]

Parameter Description

Parameter	Description
instance-id	Service instance ID, in the range from 1 to 32767.
mep-id	MEP ID, in the range from 1 to 8191.

Defaults All instances are shown by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

#Show the linktrace information of a MEP.

```
Ruijie# show cfm linktrace-info service-instance 1 mep 100
```

#Show all linktrace information of all MEPs in a service instance.

```
Ruijie# show cfm linktrace-info service-instance 1
```

#Shows all the linktrace information.

```
Ruijie# show cfm linktrace-info
```

Related Commands

Command	Description
cfm linktrace service-instance mep ttl	Enables the linktrace function.

Platform Description N/A.

show cfm ma

Use this command to show the MA configurations.

show cfm ma [*ma-name*] **md** [*md-name*]

Parameter Description

Parameter	Description
ma-name	The MA name.
md-name	The MD name.

Defaults All MAs are shown by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

#Show the MA_A_MD_A configuration of MD_A.

```
Ruijie# show cfm ma MA_A_MD_A md MD_A
```

#Show the MA configuration of MD_A.

```
Ruijie# show cfm ma md MD_A
```

#Show the MA configuration.

```
Ruijie# show cfm ma
```

Related Commands

Command	Description
cfm ma md vlan	Sets the MA.

Platform Description N/A.

show cfm md

Use this command to show the MD configuration.

show cfm md

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie# show cfm md
```

Related Commands

Command	Description
cfm md level	Sets the MD.

Platform Description N/A.

show cfm mep service-instance

Use this command to show the MEP configuration.

show cfm mep *mep-id* service-**instance** *instance-id*

Parameter Description

Parameter	Description
mep-id	MEP ID, in the range from 1 to 8191.
instance-id	Service instance ID, in the range from 1 to 32767.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie#  show cfm mep 100 service-instance 1
```

Related Commands

Command	Description
cfm mep service-instance	Sets the MEP.

Platform Description N/A.

show cfm mep-list service-instance

Use this command to show the MEP list information.

show cfm mep-list [**service-instance** *instance-id*]

Parameter Description

Parameter	Description
instance-id	Service instance ID.

Defaults All MEP lists are shown by default.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie# show cfm mep-list service-instance 1
```

Related Commands

Command	Description
cfm mep service-instance	Sets the MEP.
cfm mip-rule service-instance	Sets the MIP generation rule.

Platform Description N/A.

show cfm mp

Use this command to show the MP information.

show cfm mp [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface ID.

Defaults By default, information of MPs on all interfaces (including the MEP and MIP) are shown.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie# show mp interface gigabitethernet 1/1
```

Related Commands

Command	Description
cfm mep service-instance	Sets the MEP.
cfm mip-rule service-instance	Sets the MIP generation rule.

Platform Description N/A.

show cfm remote-mep service-instance mep

Use this command to show the remote MEP information.

show cfm remote-mep service-instance *instance-id* **mep** *mep-id*

Parameter Description

Parameter	Description
instance-id	Service instance ID, in the range from 1 to 32767.
mep-id	MEP ID, in the range from 1 to 8191.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie# show cfm remote-mep service-instance 1 mep 100
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

show cfm service-instance

Use this command to show the service instance configuration.

show cfm service-instance [*instance-id*]

Parameter Description

Parameter	Description
instance-id	Service instance ID, in the range from 1 to 32767.

Defaults

All service instances are shown by default.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

```
Ruijie# show cfm service-instance 1
```

Related Commands

Command	Description
cfm service-instance md ma	Sets a service instance.

Platform Description

N/A.

REUP Configuration Commands

link state track

Use this command to enable the link state track group. The no form of this command is used to disable a link state track group

link state track [*num*]

no link state track [*num*]

Parameter Description

Parameter	Description
num	Interface ID of the link aggregation group.

Defaults

N/A.

Command Mode

Global configuration mode.

Usage Guide

First create a link state track group and then add a port into the specified link state track group.

Configuration Examples

The following example shows how to create a link state track group:

```
Ruijie(config)# link state track 1
```

Related Commands

Command	Description
link state group	Adds the port to the specified link state track group.

Platform Description

N/A.

link state group

Use this command to add the port into the specified link state track group. The no form of this command is used to delete a port from the specified link state track group.

link state group *num* { **upstream** \| **downstream** }

no link state group

Parameter Description

Parameter	Description
num	ID of the link state track group.
upstream	Configures the port to be an upstream port in the link state track

	group.
downstream	Configures the port to be a downstream port in the link state track group.

Defaults

The port is not added into any link state track group.

Command Mode

Interface configuration mode.

Usage Guide

First create a link state track group and then add a port into the specified link state track group.

Configuration Examples

The following example shows how to add the port fa0/2 into the link state track group:

```
Ruijie(config)# link state track 1
Ruijie(config)# interface fa 0/2
Ruijie(config-if)# link state group 1 upstream
```

Related Commands

Command	Description
link state track	Enables a link state track group.

Platform Description

N/A.

mac-address-table move update max-update-rate

Use this command to configure the maximum number of MAC address update packets sent per second.

mac-address-table move update max-update-rate *pkts-per-second*

no mac-address-table move update max-update-rate

Parameter Description

Parameter	Description
pkts-per-second	The maximum number of MAC address update packets sent per second. It ranges from 0 to 32000, and the default value is 150.

Defaults

A maximum of 150 MAC address update packets are sent per second.

Command Mode

Global configuration mode.

Usage Guide

When a link is switched, REUP sends a certain number of MAC address update packets to an uplink device in every second to recover downlink data transmission of the uplink device.

Configuration Examples

The following example shows how to configure the maximum number of MAC address update packets sent per second:

```
Ruijie(config)# mac-address-table move update max-update-rate 20
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

mac-aadress-table move update receive

Use this command to enable REUP to receive the mac-address-table update messages.

mac-address-table move update receive

no mac-address-table move update receive

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

Disabled.

Command Mode

Global configuration mode.

Usage Guide

The dual link backup switchover will lead to the loss of downstream data flow, for the MAC address for the uplink switch has not been updated in time. Therefore, it is necessary to update the MAC address table of the uplink switch, to reduce the loss of L2 data flow. You need to enable the switch of receiving the MAC address update messages on the uplink switch.

Configuration Examples

```
Ruijie(config)# mac-address-table move update receive
```

Related Commands

Command	Description
mac-address-table move update transit	Enables REUP to transmit the mac-address-table update messages.

Platform Description

N/A.

mac-address-table move update receive vlan

Use this command to configure the VLANs processing MAC address update packets.

mac-address-table move update receive vlan *vlan-range*

no mac-address-table move update receive vlan *vlan-range*

Parameter Description

Parameter	Description
vlan-range	Range of the VLANs processing MAC address update packets.

Defaults All VLANs process MAC address update packets.

Command Mode Global configuration mode.

Usage Guide This command can be used to disable some VLANs from processing MAC address update packets. VLANs disabled from processing MAC address update packets can still recover downlink data transmission of the uplink device using MAC address update packets, but the capability to provide convergence on link failure will be degraded.

Configuration Examples The following example configures VLANs processing MAC address update packets:

```
Ruijie(config)# no mac-address-table move update receive vlan 20
```

Related Commands

Command	Description
mac-address-table move update receive	Enables REUP to receive MAC address update packets.

Platform Description N/A.

mac-address-table move update transit

Use this command to enable REUP to transmit the mac-address-table update messages.

mac-address-table move update transit

no mac-address-table move update transit

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults Disabled.

Command Mode Global configuration mode.

Usage Guide In order to reduce the link switchover and the loss of the downstream data flow, it is necessary to enable the switch of receiving the MAC address update messages on the uplink switch.

Configuration Examples

```
Ruijie(config)# mac-address-table move update transit
```

Related Commands

Command	Description
mac-address-table move update transit vlan	Enables REUP to transmit the mac-address-table update messages.

Platform Description

N/A.

mac-address-table move update transit vlan

Use this command to enable REUP to transmit the mac-address update messages.

mac-address-table move update transit vlan *vid*

no mac-address-table move update transit vlan

Parameter Description

Parameter	Description
vid	ID of the VLAN transmitting MAC address update packets.

Defaults

Transmit the MAC-address update messages in the default VLAN on the port.

Command Mode

Interface configuration mode.

Usage Guide

When a link is switched, the VLAN enabled to transmit MAC address update packets will send MAC address update packets to its uplink device.

Configuration Examples

The following example configures VLANs transmitting MAC address update packets:

```
Ruijie(config)# mac-address-table move update transit
```

Related Commands

Command	Description
mac-address-table move update transit	Enables REUP to receive the mac-address-table update messages.

Platform Description

N/A.

mac-address-table update group

Use this command to set the mac-address-table update group.

mac-address-table update group [*group-num*]

no mac-address-table update group

Parameter Description

Parameter	Description
group-num	The mac-address-table update group ID.

Defaults

The default group number is 1.

By default, no mac-address-table update group is configured.

Command Mode

Interface configuration mode.

Usage Guide

In order to reduce the flood due to the MAC address update and the influence on the normal data transmission of the switch, Ruijie products add a configuration of MAC address update group. Only if all the interfaces are added to a MAC address update group, the downstream data transmission be restored rapidly.

Configuration Examples

```
Ruijie(config-if)# mac-address-table update group 2
```

Related Commands

Command	Description
show mac-address-table update group detail	Shows the mac-address-table update group information.

Platform Description

N/A.

switchport backup interface *interface-id*

Use this command to configure the REUP dual link backup interface.

switchport backup interface *interface-id*

no switchport backup

Parameter Description

Parameter	Description
interface-id	Interface ID of the backup link.

Defaults

N/A.

Command Mode

Interface configuration mode.

Usage Guide

Enter the primary interface configuration mode, the interface-id in the parameter is for the backup interface. When the active link fails, the backup link transmission is restored rapidly

Configuration Examples

The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as primary interface and backup interface:

```
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# switchport backup interface fa 0/2
```

Related Commands

Command	Description
show interface switchport backup	Displays the dual link backup configuration on the switch.

Platform Description

N/A.

switchport backup interface preemption

Use this command to configure the REUP link preemption function.

switchport backup interface *interface-id* **preemption mode** { **forced** | **bandwidth** | **off** }

switchport backup interface *interface-id* **preemption delay** *delay-time*

no switchport backup interface *interface-id* **preemption delay**

Parameter Description

Parameter	Description
interface-id	The interface id of the backup link.
delay-time	The preemption delay time.

Defaults

The preemption function is disabled by default.
The default preemption delay time is 35s.

Command Mode

Interface configuration mode.

Usage Guide

The preemption mode includes **forced, bandwidth and off**. In the **bandwidth** preemption mode, the interface with high bandwidth has priority over other interfaces to transmit the data. In the **forced** preemption mode, the primary has priority over backup interfaces to transmit the data. No preemption event occurs in the **off** preemption mode. By default, the preemption mode is off.

The preemption delay refers to the delay time of the link reswitch after the restoration of the link failure.

Configuration Examples

The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as the primary interface and backup interface, set the bandwidth preemption mode and 40s preemption delay:

```
Ruijie(config)# interface fa 0/1
Ruijie(config-if)# switchport backup interface fa 0/2
preemption mode bandwitdh
Ruijie(config-if)# switchport backup interface fa 0/2
```

```
preemption delay 40
```

Related Commands

Command	Description
show interface switchport backup	Displays the dual link backup configuration.

Platform Description

N/A.

switchport backup interface prefer

Use this command to configure VLAN load balancing on a link. The no form of this command is used to delete the configured VLAN load strategy.

switchport backup interface *interface-id* **prefer instance** *instance-range*

no switchport backup interface *interface-id* **prefer**

Parameter Description

Parameter	Description
interface-id	Interface ID of the backup link.
instance-range	Instance range of loading on the backup interface.

Defaults

No VLAN load on the backup interface.

Command Mode

Interface configuration mode.

Usage Guide

MSTP instance mapping can be used to modify the mapping between an instance and a VLAN.

Configuration Examples

The following example configures VLAN load balancing on dual links.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport backup interface gigabitEthernet 0/2 prefer
instance 1
```

Related Commands

Command	Description
show interface switchport backup	Displays the configuration of dual-link backup on the switch.
spanning-tree mst configuration	Configures MSTP instances.

Platform Description

N/A.

show interfaces switchport backup

Use this command to show the dual link backup information on the interfaces.

show interfaces [*interface-id*] **switchport backup** [**detail**]

Parameter Description

Parameter	Description
interface-id	The interface id of the dual link backup.
detail	Displays the detailed information about the dual link backup.

Defaults

Show the dual link backup information on all interfaces.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

```
Ruijie # show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface     Backup Interface      State
----------------------------------------------------
Gi0/23               Gi0/24                Active Up/Backup Standby
Interface Pair : Gi0/23, Gi0/24
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi0/23(1000 Mbits), Gi0/24(1000 Mbits)
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

show link state group

Use this command to show the information of a link state track group.

show link state group *num*

Parameter Description

Parameter	Description
num	ID of a link state track group.

Defaults

N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples The following example shows the link state track group:

```
Ruijie # show link state group
Link State Group:1  Status: Enabled, UP
Upstream Interfaces :Gi0/1(Up)
Downstream Interfaces :Gi0/3(Dwn), Gi0/4(Dwn)
Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A.

show mac-address-table update group detail

Use this command to show the mac-address-table update group information.

show mac-address-table update group detail

Parameter Description

Parameter	Description
detail	Displays the detailed information about the mac-address-table update group.

Defaults Show the mac-address-table update group information.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration Examples

```
Ruijie # configure terminal
Ruijie (config)# mac-address-table move update receive
Ruijie (config)# interface range gigabitEthernet 0/3-4
Ruijie (config-if-range)# mac-address-table update group
Ruijie (config-if-range)# end
Ruijie # show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:7
Group member  Receive Count  Last Receive Switch-ID  Receive Time
----------------------------------------------------------
GigabitEthernet 0/3  0             0000.0000.0000
GigabitEthernet 0/4  0             0000.0000.0000
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

RLDP Configuration 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

Parameter	Description

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

Command	Description

Commands

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 Description N/A.

TPP Configuration Commands

show tpp

Use this command to show the configuration of topology protection.

show tpp

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 current TPP configuration and port detection.

Configuration Examples The following example shows how to display information about the topology protection function:

```
Ruijie# show tpp
```

Related Commands

Command	Description
topology guard	Enable the topology protection function globally.

Platform Description N/A.

topology guard

In global configuration command mode, use this command to enable the topology protection function. Use the **no** form of this command to disable the topology protection function.

topology guard

no topology guard

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults Enabled.

Command Mode

Global configuration mode.

Usage Guide

The topology protection function is enabled by default, so as to protect the network against topology oscillation due to attacks. It should be used with the **cpu topology-limit** command.

Configuration Examples

The following example shows how to enable and disable the global topology protection function:

```
Ruijie(config)# topology guard
Ruijie(config)# no topology guard
```

Related Commands

Command	Description
tp-guard port enable	Enable the topology protection function on the interface.
cpu topology-limit	Set the CPU utilization limitation.

Platform Description

N/A.

tp-guard port enable

Use this command to enable the topology protection function on the port. Use the **no** form of this command to disable the function.

tp-guard port enable

no tp-guard port enable

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

N/A.

Command Mode

Interface configuration mode.

Usage Guide

If both the global topology protection function and the topology protection function of the port are enabled, the remote device of this port will be notified when the CPU utilization of the local device is too high or there are other problems with the local device. This command is applicable to the layer 2 switching interfaces and routing interfaces. Other interfaces (including AP member port) do not support this command.

Configuration Examples

The following example shows how to configure the topology protection function for the port:

```
Ruijie(config-if)# tp-guard port enable
Ruijie(config-if)# no tp-guard port enable
```

Related Commands

Command	Description
topology guard	Enable the topology protection function globally.

Platform Description

N/A.

BFD Configuration Commands

bfd

Use this command to set the BFD session parameter 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

Parameter Description

Parameter	Description
interval *milliseconds*	Interval of sending the BFD control messages to the BFD session neighbor. *milliseconds*: valid range from 50 ms to 10000 ms.
min_rx *milliseconds*	Expected interval of receiving the BFD control messages from the BFD session neighbor. *milliseconds*: valid range from 50 ms to 10000 ms.
multiplier *multiplier-value*	Count of BFD control message not received from the peer in the configured interval. *multiplier-value*: valid range from 3 to 50.

Defaults

No BFD session parameters by default. Those parameters must be configured before enabling the BFD session.

Command Mode

Interface configuration mode.

Usage Guide

The express forwarding must be enabled before enabling BFD on the routers.

Configuration Examples

The following example shows how to configure the BFD session parameter on Routed Port FastEthernet 0/2:

```
Ruijie(config)# interface fastEthernet 0/2
Ruijie(config)# no switchport
Ruijie(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

Related Commands

Command	Description
bfd all-interfaces	Configure BFD for all route protocols on the interface.
ip ospf bfd	Configure BFD for OSPF.
ip rip bfd	Configure BFD for RIP.

Platform Description N/A

bfd cpp

Use this command to enable the BFD protection policy in global configuration command. 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 Enabled.

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

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 the 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	BFD slow-timer time, ranging from, 1000 to 30000 and the default value is 1000. The unit is millisecond.

Defaults 1000 ms.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The example below sets the slow-timer as 14000 ms:

```
Ruijie(config)# bfd slow-timer 14000
```

Related Commands

Command	Description
bfd echo	Enable the BFD echo function

Platform Description N/A

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	Set the bfd up-dampening time, ranging from 0 to 300000. The unit is millisecond.

Defaults 0 ms, which means that the session state is UP and notifying the application level of the state change immediately.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The example below sets the bfd up-dampening time as 60000 ms:

```
Ruijie(config)# bfd up-dampening 60000
```

Related Commands

Command	Description
bfd	Configure the BFD session parameter.

Platform Description

N/A

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 *interface-type interface-number gateway* [**source** *ip-address*]

no ip route static bfd *interface-type interface-number gateway* [**source** *ip-address*]

Parameter Description

Parameter	Description
interface-type *interface-number*	Set the interface type and interface number.
gateway	Set 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) set 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 configuration of BFD for the static route.

Command Mode

Global configuration mode.

Usage Guide

Note that the BFD session parameters must have been configured before the configuration.

Configuration Examples

The example below 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
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)# exit
Ruijie(config)# ip route static bfd FastEthernet 0/1 172.16.0.2
Ruijie(config)# ip route 10.0.0.0 255.0.0.0 FastEthernet 0/1 172.16.0.2
```

Related Commands

Command	Description

bfd	Set the BFD session parameters.

Platform Description

N/A

show bfd neighbors

Use this command to show the BFD session parameters.

show bfd neighbors [**client static-route**] [**ipv4** *ip-addess* | **ipv6** *ip-addess*] [**details**]

Parameter Description

Parameter	Description
client	(Optional) specify the routing protocol.
static-route	Show the BFD session configuration for the static route.
ipv4 *ip-address*	(Optional) Show the session information of the specified IPv4 neighbor.
ipv6 *ip-address*	(Optional) Show the session information of the specified IPv6 neighbor.
details	(Optional) Show the configurations in detail.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

In the information displayed by the **show bfd neighbors** command, the OurAddr field means the source address of the session.

Configuration Examples

#The following 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 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	Descripton
OurAddr	Local IP address.
NeighAddr	Neighbor IP address.
LD/RD	Local & Remote identifiers.
RH/RS	Whether the remote session responses the local session.
Holdown(mult)	Time of not receiving the hello packets for the local session and the times of the timeout detection.
State	The current session state.
Int	The interface number for the session.
Session state is UP and using echo function with 50 ms interval	Whether the session is in the echo mode and the echo interval (which is shown only in the echo mode).
Local Diag	Session diagnostic information.
Demand mode	Whether the session poll mode is active or not.
Poll bit	Whether the session configuration has been modified or not.
MinTxInt	The minimum sending interval for the local session.
MinRxInt	The minimum receiving interval for the local session.
Multiplier	The timeout detection times for the local session.
Received MinRxInt	The minimum sending interval for the remote session.
Received Multiplier	The timeout detection times for the remote session.
Holdown (hits)	The session detection time and the times of the timeout detection.
Hello (hits)	The minimum interval of receiving the hello packets after the session negotiation.
Rx Count	The number of BFD packets received by the local session.
Rx Interval (ms)	The minimum, maximum and

min/max/avg	average intervals of receiving for the local session.
Tx Count	The number of BFD packets sent by the local session.
Tx Interval (ms) min/max/avg	The minimum, maximum and average intervals of sending for the local session.
Registered protocols	The registered protocol type of the session.
Uptime	The time of keeping the session UP.
Last packet	The last BFD packet information received by the local session.

Related Commands

Command	**Description**
N/A	N/A

RNS&Track Configuration Commands

delay

Use this command to specify a period of time after which the track object status will change if the interface status changes.

delay { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }

Parameter Description

Parameter	Description
seconds	Set the delay time. The unit is second.

Defaults No delay by default.

Command Mode Track configuration mode.

Usage Guide The continual oscillation of the track object status may cause its client to change as well. This command can be used to delay advertising the change of the track object status. For example, the status of a track object changes from up to down, if the **delay down** 180 command is configured, the down status will be advertised after 180 seconds. If the track object status changes to the up again in this period, it will not be advertised. For the client of the track object, the status of the track object is always up.

Configuration Examples Delay 30 seconds to advertise after the track object status changes from down to up.

```
Ruijie(config-track)# delay up 30
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description N/A.

dns name-server

Use this command to set an iprns object to send the dns packets and to enter the ip rns dns mode.

dns *word* **name-server** *a.b.c.d*

Parameter Description

Parameter	Description

word	Set the destination IP address or the destination host domain name.
a.b.c.d	Set 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.

Configuration Examples

```
Ruijie(config-ip-rns)# dnswww.ruijie.com.cnname-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 more than or equal to the timeout time.

frequency *milliseconds*

Parameter Description

Parameter	Description
milliseconds	Set the interval of sending the packets, in the range of 10 to 604800000.

Defaults

60s.

Command Mode

ICMP echo configuration mode/DNS configuration mode.

Usage Guide

Use this command to set the interval of sending the icmp echo or dns packets, which must be more than or equal to the timeout time configured. It is recommended not to set this value too small, which may put great pressure to the CPU.

Configuration Examples

N/A.

Related Commands

Command	Description

timeout	Define the timeout time of sending the packets.

Platform Description

N/A

icmp-echo

Use this command to set an ip rns object to send the icmp echo packets and to enter the ip rns icmp echo configuration mode.

icmp-echo *destination-hostname* [**source-ipaddr** *ip-address*]

Parameter Description

Parameter	**Description**
destination-hostname	Set the destination IP address for the ICMP echo packets.
ip-address	(Optional) Set the source IP address for the ICMP echo packets.

Defaults

N/A.

Command Mode

IP RNS configuration mode.

Usage Guide

This command enables ip rns object to send icmp echo packets and the destination ip address is the ip address configured by the user.

Configuration Examples

```
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
```

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. The **no** form of this command is used to delete an ip rns object

ip rns *operation-number*

no ip rns *operation-number*

Parameter Description

Parameter	**Description**
operation-number	Set the ip rns operation object number, in the range of 1 to 700.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

Use this command to enter the ip-rns configuration mode, where you can configure to send icmp packets and to send dns request packets.

Configuration Examples

The following example defines the ip rns object 1.

```
Ruijie(config)#ip rns1
```

Related Commands

Command	Description
show ip rns statistics	Show the statistical data on the ip rns object.

Platform Description

N/A

show iprns configuration

Use this command to show the RNS object configurations.

show ip rns configuration [*operation-number*]

Parameter Description

Parameter	Description
operation-number	Set the ip rns operation object number, in the range of 1 to 700.

Defaults

N/A.

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to show a specific RNS object configuration. The configuration information varies with the packet type.

Configuration Examples

N/A.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show ip rns statistics

Use this command to show the RNS object statistical information.

show ip rns statistics [*operation-number*]

Parameter Description

Parameter	Description
operation-number	Set the ip rns operation object number, in the range of 1 to 700.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to show the statistical information of a specific RNS object. The statistical information varies with the packet type.

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

show track

Use this command to show the statistical information of the track object

show track [*track-number*]

Parameter Description

Parameter	Description
track-number	Set the track object number, in the range of 1-700.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to show the statistical information of a specific Track object.

Configuration N/A

Examples

Related Commands

Command	**Description**
N/A.	N/A.

Platform Description N/A.

timeout

Use this command to set the timeout time of sending the packets.

timeout *milliseconds*

Parameter Description

Parameter	**Description**
milliseconds	Set the timeout time, in ms.

Defaults By default, the timeout time of sending the icmp echo packets is 5s; the timeout time of sending the dns packets is 9s.

Command Mode ICMP echo configuration mode/DNS configuration mode.

Usage Guide Use this command to configure the timeout time for packets. If no packets are received within this period of time, the device will regard that no response packets are received.

Configuration Examples N/A.

Related Commands

Command	**Description**
frequency *milliseconds*	Set the interval of sending the packets.

Platform Description N/A.

track interface line-protocol

Use this command to configure a track object to track the interface status and enter the track mode. The **no** form of this command is used to delete a track object.

track *object-number* **interface** *type number* **line-protocol**

no track *object-number*

Parameter Description

Parameter	Description
object-number	Set the track object number, in the range of 1 to 700.
type number	Set the interface type and the interface number.

Defaults N/A.

Command Mode Global configuration mode

Usage Guide Use this command to configure a track object to track the link status of the interface. If the link status of the interface is up, the status of the corresponding track object is up too.

Configuration Examples

```
Ruijie(config)# track 3 interface ethernet 0/1 line-protocol
```

Related Commands

Command	Description
track object-number rns entry-number	Configure a track object to track the operating status of an rns object.
show track	Show the track object related information.

Platform Description N/A.

track rns

Use this command to configure a track object to track the operating status of an rns object and enter the track mode. The **no** form of this command is used to delete a track object.

track *object-number***rns** *entry-number*

no track *object-number*

Parameter Description

Parameter	Description
object-number	Set the track object number, in the range of 1 to 700.
entry-number	Set the RNS object number, in the range of 1 to 700.

Defaults N/A.

Command Mode Global configuration mode

Usage Guide The rnd object status is determined by whether the response packets are received. If so, the rns object status is up and the status of the corresponding track object that tracks this rns is also up.

Configuration Examples

```
Ruijie(config)# track 123 rns 1
```

Related Commands

Command	Description
track interface line-protocol	Track the status of one interface and enter the track mode.
show track [*track-number*]	Show the track object related information.

Platform Description

N/A.

GRTD Configuration Commands

diagnostic bootup level

Use this command to set the bootup test level in global configuration mode: bypass bootup test, minimal bootup test, and complete bootup test.

diagnostic bootup level {**bypass | minimal | complete**}

Parameter description

Parameter	Description
bypass	Bypass bootup test
minimal	Minimal bootup test
complete	Complete bootup test

Default

The default level is **minimal**.

Command mode

Global configuration mode

Usage guidelines

Use the **diagnostic bootup level** command to set the bootup test level.

Three levels of bootup test can be configured: bypass bootup test, minimal bootup test, and complete bootup test.

⚠ **Caution**	The configured bootup test level takes effect during the next reset process instead of taking effect immediately after being configured.

Examples

Example 1: The following example sets the bootup test level as complete bootup test:

```
ruijie(config)#diagnostic bootup level complete
ruijie(config)#
```

Example 2: The following example recovers the bootup test level.

```
ruijie(config)#no diagnostic bootup level
ruijie(config)#
```

Field	Description
complete	Complete bootup test

Related commands

Command	Description
show diagnostic bootup level	Show the current bootup test level.

Platform description

N/A

diagnostic event-log size

Use this command to set the number of diagnostic event records in global configuration mode, ranging from 1 to 1000.

diagnostic event-log size *size-value*

no diagnostic event-log size

Parameter description

Parameter	Description
size-value	Number of diagnostic event records

Default

The default number of diagnostic event records is 500.

Command mode

Global configuration mode

Usage guidelines

Use the **diagnostic event-log size** command to set the number of diagnostic event records.

You can set the number of diagnostic event records to 1-1000.

⚠ **Caution**

This command is for the host only. All diagnostic events on modules are stored on the host.

Examples

Example 1: The following example sets the number of diagnostic event records to 1000.

```
ruijie(config)#diagnostic event-log size 1000
ruijie(config)#
```

Example 2: The following example sets the number of diagnostic event records to the default value.

```
ruijie(config)#no diagnostic event-log size
ruijie(config)#
```

Field	Description
size-value	The number of event records to be set

Related commands

Command	Description
show diagnostic events	Show diagnostic events.

Platform description

N/A

diagnostic loopback-test

As an exclusive command for port testing in privileged EXEC mode, this command is used to set the parameter for port setting, including port ID and port loopback mode.

diagnostic loopback-test [**slot** *slot_id* [**sub_system** *subsys_id*]] **port** {**all** | **range** *port_range* | port_id} **loopback** {**mac | phy | none**}

Parameter description

Parameter	Description
range_value	Port No.: The format is 1/1-24. The number 1 before the forward slash is slot ID.
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to *cpu id* in the **show version** command.
mac	Port MAC loopback
phy	Port PHY loopback
none	Cancelling port loopback

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Use the **diagnostic loopback-test** command to set the port ID and port loopback mode for port setting.

Examples

Example 1: The following example tests ports 1-10 of module 1 without setting loopback, with loopback implemented through a loopback adapter. Suppose that the test item ID in this module is 5.

```
ruijie# diagnostic loopback-test slot 1 port range
1-10 loopback no
ruijie# diagnostic start slot 1 test 5
```

Related commands

Command	Description
None	

Platform description

N/A

diagnostic monitor active

Use this command to set the health monitoring test status for a test item of a particular module in global configuration mode: **active** or **inactive**.

diagnostic monitor active [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **|** **range** *test-range*}

no diagnostic monitor active [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** **|** *test-id* **|** **range** *test-range*}

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to *cpu id* in the **show version** command.
test{**all** **|** *test-id* | **range** *test-range*}	Test items. **all** means all items; **range** means a range, for example, from item m to item n.

Default

Active

Command mode

Global configuration mode

Usage guidelines

Use the **diagnostic monitor active** command to set the health monitoring test status for a test item of a particular module.

You can set the health monitoring test status for a test item of a particular module to **active** or **inactive**.

⚠ **Caution**	The health monitoring test status for a destructive test cannot be set to **active**. You can view the attributes of test items of modules by using the **show diagnostic content** command.

Examples

Example 1: The following example sets the health monitoring test status of items 1-4 of module 2 to **active**.

```
ruijie(config)#diagnostic monitor active slot 2 test range
1-4
ruijie(config)#
The test:1 can not be used as health monitoring test
```

Example 2: The following example sets the health monitoring test status of all test items 1-4 of a BOX device to **inactive**.

```
ruijie(config)#no diagnostic monitor active test all
ruijie(config)#
```

Field	Description
slot **2** test range **1-4**	Items 2-4 of slot 2

Related commands

Command	Description
show diagnostic content	Show diagnostic test information.

Platform description

N/A

diagnostic monitor interval

Use this command to set the test interval for system health monitoring in global configuration mode, with the second as the minimum unit.

diagnostic monitor interval [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all |** *test-id* **| range** *test-range*} *hh:mm:ss* **day** *day_count*

no diagnostic monitor interval [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **| range** *test-range*}

Parameter description

Parameter	Description
slot *slot_id*	(Optional) Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to *cpu id* in the **show version** command.

test {**all |** *test-id* **|range** *test-range*}	Test items. **all** means all items; **range** means a range, for example, from item m to item n.
hh:mm:ss	Hour:minute:second, for example, 00:00:40
day_count	Number of days

Default

The default interval for ping tests is 20s.

Command mode

Global configuration mode

Usage guidelines

Use the **diagnostic monitor interval** command to set the monitoring interval for a specified test item in a module.

The number of days ranges from 0 to 20.

⚠ **Caution**	The destructive test cannot be a test item for system health monitoring, so the test interval for destructive tests cannot be set. You can view the attributes of test items of slots or management boards by using the **show diagnostic content** command.

Examples

Example 1: The following example sets the second test item of a BOX device to the health monitoring test item, with 12:12:12 100 subseconds of every 10th day as the test interval.

```
ruijie(config)#diagnostic monitor interval test 2 12:12:12 day 10
ruijie(config)#
```

Example 2: The following example sets the health monitoring test interval of the second test item of slot 2 back to the default value.

```
ruijie(config)#no diagnostic monitor interval slot 2 test 2
ruijie(config)#
```

Field	Description
slot **2** test **2**	The second test item of slot 2
12:12:12 day **10**	12 o'clock 12 minutes 12 seconds, with the number of days being 10

Related commands

Command	Description
show diagnostic content	Show diagnostic test information.

Platform description

N/A

diagnostic monitor syslog

Use this command to set a system log message to be generated when any monitoring test fails.

diagnostic monitor syslog

no diagnostic monitor syslog

Parameter description

Parameter	Description
syslog	System log message

Default

By default, a system log message is generated when any monitoring test fails.

Command mode

Global configuration mode

Usage guidelines

Use the **diagnostic monitor syslog** command to set a system log message to be generated when any monitoring test fails.

Examples

Example 1: The following example sets a system log message to be generated when any monitoring test fails.

```
ruijie(config)# diagnostic monitor syslog
ruijie(config)#
```

Example 2: The following example sets no system log message to be generated when any monitoring test fails.

```
ruijie(config)#no diagnostic monitor syslog
ruijie(config)#
```

Field	Description
syslog	System log message

Related commands

Command	Description
None	

Platform description

N/A

diagnostic monitor threshold

Use this command to set the maximum number of consecutive failed health monitoring tests for some test items of a particular module in global configuration mode. For example, if you set the maximum number of consecutive failed health monitoring tests for a test item of a slot to 10, the background no longer conducts monitoring tests for this test item after 10 consecutive failed tests.

diagnostic monitor threshold [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **|** **range** *test-range*} **failure-count** *count-value*

no diagnostic monitor threshold [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **|** **range** *test-range*}

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to *cpu id* in the **show version** command.
test {**all** **|** *test-id* | **range** *test-range*}	Test items. **all** means all items; **range** means a range, for example, from item m to item n.
failure-count *count-value*	Maximum number of consecutive failed tests

Default

The maximum number of consecutive failed tests for all monitoring test items is **10** by default.

Command mode

Global configuration mode

Usage guidelines

Use the **diagnostic monitor threshold** command to set the maximum number of consecutive failed health monitoring tests for some test items of a particular module.

The maximum number of consecutive failed tests ranges from 1 to 99.

⚠ **Caution**	The destructive test cannot be a test item for system health monitoring, so the maximum number of consecutive failed tests for destructive tests cannot be set. You can view the attributes of test items of module by using the **show diagnostic content** command.

Examples

Example 1: The following example sets the maximum number of consecutive failed health monitoring tests for all test items of module 2 to **50**.

```
ruijie(config)#diagnostic monitor threshold slot 2 test all
failure-count 50
ruijie(config)#
The test:1 can not be used as health monitoring test
The test:5 can not be used as health monitoring test
......
```

Example 2: The following example sets the maximum number of consecutive failed health monitoring tests for all test items of a BOX device back to the default value.

```
ruijie(config)#no diagnostic monitor threshold test all
ruijie(config)#
```

Related commands

Command	Description
show diagnostic content	Show diagnostic test information.

Platform description

N/A

diagnostic packet

As a command for testing all packets in privileged EXEC mode, this command is used to set the length of the test packet, number sent test frames, and timeout time for receiving test frames, with tick as timeout time unit.

diagnostic packet [**slot** *slot_id* [**sub_system** *subsys_id*]] [**length** *lengtn_size*] [**num** *num_count*] [**time_out** *tick_count*]

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.
length	(Optional) Length of test frame
num	(Optional) Number of test frames
time_out	(Optional) Timeout time for receiving test frames

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Use the **diagnostic packet** command to set related parameters related to test frames.

This command is for test items for designing test frame receiving and sending, such as port loopback test and channel test.

Examples

Example 1: The following example sets the test frame parameters of slot 1.

```
ruijie# diagnostic packet slot 1 length 800 num 100 time-out 100
ruijie#
```

Related commands

Command	Description
None	

Platform description

N/A

diagnostic schedule

Use this command to set the planned timetable for some test items of a particular module in global configuration mode. For example, you can set a test item of a slot to be conducted at 12:12 on January 20, 2010 or at a fixed time each day or each week.

diagnostic schedule [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **| range** *test-range*} {**daily** *hh:mm* **|** **on** *year month day_of_month hh:mm*| **weekly** *day_of_week hh:mm*}

no diagnostic schedule [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **| range** *test-range*} {**daily** *hh:mm* **|** **on** *year month day_of_month hh:mm*| **weekly** *day_of_week hh:mm*}

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to *cpu id* in the **show version** command.
daily	Tests conducted every day. *hh:mm* indicates the test start time each day.

weekly	Tests conducted every week. *day_of_week* indicates a day in a week. *hh:mm* indicates the test start time on the day.
on	Tests conducted at a specified time on a certain day in a certain month in a certain year.

Default

The planned timetable for all test items is null.

Command mode

Global configuration mode

Usage guidelines

Use the **diagnostic schedule** command to set the planned timetable for some test items of a particular management board or slot.

- Tests can be set to be conducted sometime in a day in the future.
- Tests can be set to be conducted at a fixed time each day.
- Tests can be set to be conducted sometime in a day each week.
- The test time for some test items may be contradictory, and these test items cannot be tested at the same time.

⚠ **Caution**	If you set a test plan at a certain time, you cannot other test plans at this time.

Examples

Example 1: The following example sets items 1 and 2 of module 2 to be conducted at 10:10 a.m. each day.

```
ruijie(config)# diagnostic schedule slot 2 test range 1-2 daily 10:10
ruijie(config)#
```

Example 2: The following example sets item 1 of module 2 to be conducted at 10:10 a.m. on September 10, 2010.

```
ruijie(config)# diagnostic schedule slot 2 test 1 on 2010 9 10 10:10
ruijie(config)#
```

Example 3: The following example sets item 1 of module 2 to be conducted at 10:10 a.m. on Wednesdays.

```
ruijie(config)#diagnostic schedule slot 2 test 1 weekly wednesday 10:10
ruijie(config)#
```

Example 4: The following example cancels the planned timetable for item 1 of module 2: 10:10 a.m. on Wednesdays.

```
ruijie(config)#no diagnostic schedule slot 2 test 1 weekly
wednesday 10:10
ruijie(config)#
```

Field	Description
on	Conduct tests at a future time.
daily	Conduct tests at a fixed time each day.
weekly	Conduct tests at a fixed time each week.

Related commands

Command	Description
show diagnostic schedule	Show the planned test timetable.

Platform description

N/A

diagnostic start

Use this command to start command line tests.

diagnostic start [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **|** range *test-range*}

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.
test {**all** **|** *test-id* | **range** *test-range*}	Test items. **all** means all items; **range** means a range, for example, from item m to item n.

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Use the **diagnostic start** command to start command line tests.

Generally, in command line tests, non-destructive tests are conducted before destructive tests.

Store tests on a slot need to be conducted those on a management board, because, after store tests on a management board are conducted, the management board needs to be reset to make the system be used normally.

Caution	Before command line tests are started, you need to stop system health monitoring tests and planned tests about to be conducted.

Examples

Example 1: The following example starts the tests for all test items of module 2.

```
ruijie#diagnostic start slot 2 test all
Running test(s)1,5-11,13-15,17-26 may disrupt normal
system
Do you want to continue? [no]:yes
ruijie#
```

Related commands

Command	Description
show diagnostic result	Show the results of command line tests.

Platform description

N/A

diagnostic stop

Use this command to stop diagnostic tests of a particular module or slot in privileged EXEC mode.

diagnostic stop [**slot** *slot_id* [**sub_system** *subsys_id*]]

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

N/A

Examples

Example 1: The following example stops the command line diagnostic test of module 5.

```
ruijie#diagnostic stop slot 5
ruijie#
```

Related commands

Command	Description
None	

Platform description

N/A

show diagnostic bootup

Use this command to display the bootup test level in privileged EXEC mode.

show diagnostic bootup level

Parameter description

Parameter	Description
level	Bootup test level

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Use the **show diagnostic bootup** to display the bootup test level.

Examples

Example 1: Use the **show diagnostic bootup level** command to display the following:

```
ruijie#show diagnostic bootup level
Current bootup diagnostic level: Complete
ruijie#
```

Related commands

Command	Description

Platform description

N/A

show diagnostic content

Use this command to display diagnostic test information of a particular module in privileged EXEC mode, including all test items, attributes of test items, and configuration of test items of the management board or slot.

show diagnostic content [**slot** *slot_id* [**sub_sysytem** *subsys_id*]]

Parameter description

Parameter	Description
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.
slot *slot_id*	Slot ID

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Note	You can use the **show module** command to display module information.

Examples

Example 1: The following example displays diagnostic information of module 1:

```
Ruijie# show diagnostic content slot 1/0
***************************************************************
*****
*Diagnostic test suite attributes:
M/C*/-Minimal bootup level test / Complete bootup level test / NA
P/V*/-Per port test / Per device test / NA
D/N*/-Disruptive test / Non-disruptive test / NA
  X*/-Not a health monitoring test / NA
  F*/-Fixed monitoring interval test / NA
  E*/-Always enabled monitoring test / NA
A/I*/-Monitoring in active / Monitoring in inactive / NA
Y/O*/-Key test / Non-key test / NA
  B*/-Basic ondemand test / NA
  R*/-Power-down line cards and need reload mainbord / NA
  K*/-Require resetting the line card after the test completed /
NA
```

```
***************************************************************
*****
                                          test interval  Thre-
ID   Test Name                        Attributes  day hh:mm:ss
shold
===  ===============================  ==========  ============
====
 1)  PortLoopbackTest--------------->  MPDX*******  not  config
N/A
 2)  MacSelfTest-------------------->  C*DX*******  not  config
N/A
 3)  TestCpld----------------------->  C*DX*******  not  config
N/A
 4)  TestNandFlash------------------>  **DX*******  not  config
N/A
 5)  TestNorFlash------------------->  **DX*******  not  config
N/A
 6)  TestI2C------------------------>  C*DX*******  not  config
N/A
 7)  TestPCI------------------------>  C*DX*******  not  config
N/A
 8)  TestDdr------------------------>  **DX****B**  not  config
N/A
Ruijie#
```

Field	Description
ID	Test item ID
Test Name	Test item name
Attributes	Test item attributes. For detailed description, refer to the *Configuration Guide*.
test interval	Test interval, used for system health monitoring test
threshold	Maximum number of consecutive failed monitoring tests

Related

Command	Description

commands

diagnostic monitor interval	Set monitoring interval.
diagnostic monitor threshold	Set the maximum number of consecutive failed monitoring tests.

Platform description

N/A

show diagnostic description

Use this command to display detailed descriptions of test items in privileged EXEC mode, mainly describing the meanings of test items.

show diagnostic description [**slot** *slot_id* [**sub_system** *subsys_id*]] **test** {**all** | *test-id* **|** **range** *test-range*}

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.
test {**all** **|** *test-id* **|** **range** *test-range*}	Test items. **all** means all items; **range** means a range, for example, from item m to item n.

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Use the **show diagnostic description** command to display detailed descriptions of test items.

Examples

Example 1: The following example shows the detailed description of item 1 of module 2.

```
ruijie#show diagnostic description slot 2 test 1
TestLoopback:
This test verifies the data path between the mainboard and network
        ports of a line card.
ruijie#
```

Example 2: The following example shows the detailed descriptions of all test items of module 2.

```
ruijie#show diagnostic description slot 2 test all
PortLoopbackTest :
      This test verifies the data path between the
device and network ports.
      The test packet is looped back[mac or phy] in
the target port and flooded back onto the bus/fabric.
  MacSelfTest :
      This test verifies the cpu can operate the mac
chip exactly or not.
  TestCpld :
      This test verifies the cpld work exactly or not.
  TestNandFlash :
      This test verifies the NandFlash work exactly
or not.
  TestNorFlash :
      This test verifies the NorFlash work exactly or
not.
  TestI2C :
      This test verifies the i2c bus work exactly or
not.
  TestPCI :
      This test verifies the pci bus work exactly or
not.
  TestDdr :
      This test verifies the ddr work exactly or not.
      But some ddr failure is difficult to diagnose
only through write and read.
      On this condition, you must try some other
methods, such as high temperature test...
Ruijie#
```

Related commands

Command	Description
None	

Platform description

N/A

show diagnostic events

Use this command to display all event information generated by GRTD.

show diagnostic events [**slot** *slot_id* [**sub_system** *subsys_id*]]

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Use the **show diagnostic events** command to display all event information generated by GRTD.

Examples

Example 1: Use the **show diagnostic events** command to display the following:

```
ruijie# show diagnostic events slot 3/0
Diagnostic events <storage for 500 events, 1 events
recorded>
  Event Type (ET): I - Info, W - Warning, E - Error
  Time Stamp         ET  Slot  Event Message
  -------------------          --          ----
--------------------------
  2012-06-15 16:34:39  I   3/0   Diagnostic Pass
Ruijie#
```

Field	Description
Time Stamp	Test time
ET	Event type
Slot	Slot number
Event Message	Event message content

Related commands

Command	Description
diagnostic event-log size	Set the number of event records.

Platform description

N/A

show diagnostic result

Use this command to display all diagnostic test results in privileged EXEC mode.

show diagnostic result [**slot** *slot_id* [**sub_system** *subsys_id*]] [**test** {**all** | *test-id* **|** **range** *test-range*}]

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.
test {**all** **|** *test-id* **|** **range** *test-range*}]	(Optional) Test item

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

N/A

Examples

Example 1: Use the **show diagnostic result slot 2** command to display the following:

```
Ruijie#sho dia result  slot 3/0 t a
Current bootup diagnostic level: minimal
Overall Diagnostic Result for Module: PASS
Test result: (P = Pass, F = Fail, U = Untested)
 1) PortLoopbackTest(loop mode: Mac):
    slot 0 port  1  2  3  4  5  6  7  8  9 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25
                 P  P  P  P  P  P  P  P  P  P  P  P  P  P
P  P  P  P  P  P  P  P  P  P  P
                 26 27 28 29 30 31 32 33 34 35 36 37 38
39 40 41 42 43 44 45 46 47 48
                  P  P  P  P  P  P  P  P  P  P  P  P  P
```

```
P  P  P  P  P  P  U  P  U  U
 2)
MacSelfTest------------------------------------> U
 3)
TestCpld---------------------------------------> U
 4)
TestNandFlash----------------------------------> U
 5)
TestNorFlash-----------------------------------> U
 6)
TestI2C----------------------------------------> U
 7)
TestPCI----------------------------------------> U
 8)
TestDdr----------------------------------------> U
Ruijie#
```

Related commands

Command	Description
None	

Platform description

N/A

show diagnostic schedule

Use this command to display the planned test timetables for modules in privileged EXEC mode.

show diagnostic schedule [**slot** *slot_id* [**sub_system** *subsys_id*]]

Parameter description

Parameter	Description
slot *slot_id*	Slot ID
sub_system *subsys_id*	(Optional) Subsystem ID (value range: 0-1), whose meaning is equivalent to cpu id in the show version command.

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

N/A

Examples

Example 1: Use the **show diagnostic schedule slot all** command to display the following:

```
Ruijie#sho diagnostic schedule slot 1/0
Schedule #1:
   To be run on daily 12:00
   Test ID(s) to be executed : 1 2 3 4 5 6 7 8
Schedule #2:
   To be run on June 15 2012 19:00
   Test ID(s) to be executed : 1
Ruijie#
```

Related commands

Command	Description
diagnostic schedule	Set the planned test timetables for modules.

Platform description

N/A

show diagnostic status

Use this command to display all current diagnostic test status in privileged EXEC mode.

show diagnostic status

Parameter description

Parameter	Description
status	Current test status

Default

This command has no default setting.

Command mode

Privileged EXEC mode

Usage guidelines

Use the **show diagnostic status** command to display all current diagnostic test status.

Examples

Example 1: Use the **show diagnostic status** command to display the following:

```
Ruijie#sho dia status
  (BU)-Bootup Diagnostics, (HM)-Health Monitoring
Diagnostics,
  (OD)-OnDemand    Diagnostics,    (SCH)-Scheduled
Diagnostics
  ===      ====      ==============================
======================== ======
  Dev  Slot  Description                    Current
Running Test    Run by
  ---      ----      ------------------------------
------------------------ ------
  1    0     S5750-48GT/4SFP-E                  N/A
N/A
  3    0     RG-S5750-48GT/4SFP-E               N/A
N/A
  ===      ====      ==============================
======================== ======
Ruijie#
```

Field	Description
Slot	Slot ID, and the 0 indicates the host.
Dev	Device ID
Description	Module name
Current Running Test	Running test item
Run by	Diagnostic mode

Related commands

Command	Description
None	

Platform description

N/A

SEM Configuration Commands

action cli

In SEM configuration mode, use this command to configure the policy action that executes the command line. The **no** form of this command deletes the action with the specified label.

action *label* **cli command** *cli-string* [**pattern** *pattern-string*]

no action *label*

Parameter description

Parameter	Description
label	Label of the action.
command *cli-string*	Command to be executed.
pattern *pattern-string*	(optional) Response pattern when the command string solicits input.

Default configuration

By default, no action is configured.

Command mode

SEM configuration mode

Usage Guideline

The policy executes command in the user mode, so the first command executed is "enable" to enter the privilege mode. No password is required from the user in action cli; you will pass authentication directly.

Pattern-string contains multiple response messages segmented by spaces. In case there is space in the response message, use "" to combine the response messages.

The command outputs generated by executing the action can be recorded into the device file system. Enable recording by executing policy record and configure the size of log file. Execute smart manager policy record clean command to clear the command output records generated. Please refer to the command of policy record for details.

Examples

Example 1: Create a none event executed by smart manager run as clear_cache, which will clears the arp table and IP routing table and notify the user upon completion of action.

```
Ruijie(config)#smart manager applet clear_cache
Ruijie(config-applet)#event tag monitor_cmd none
Ruijie(config-applet)#action 00 cli command "enable"
Ruijie(config-applet)#action 10 cli command "clear arp-cache"
Ruijie(config-applet)#action 20 cli command "clear ip route *"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.
policy record	Configure the size for recording CLI action outputs.
smart manager policy record	Clear CLI records generated during the execution of SEM policy.

Platform description

N/A

action counter

In SEM configuration mode, use this command to configure the policy action that operates the SEM counter. The **no** form of this command deletes the action with the specified label.

action *label* **counter name** *counter-name* **value** *counter-value* **op** {**dec** | **inc** | **nop** | **set**}

no action *label*

Parameter description

Parameter	Description
label	Label of the action
name *counter-name*	Name of the operated counter.
value *counter-value*	Numerical value used in the operation.
op { dec | inc nop |set }	Method used in the operation.

Default configuration

By default, no action is configured.

Command mode

SEM configuration mode

Usage Guideline

The counter specified in the parameter **name** *counter-name* can be used immediately without the need of definition.

Examples

Example1: if the login faile occurs in the syslog during the monitoring, add 1 to the counter Authenticate_Faile.

```
Monitor the log, if the content of the login faile
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_log syslog pattern "login
faile"
Ruijie(config-applet)#action 00 counter name Authenticate_Faile op
inc value 1
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

action exit

In SEM configuration mode, use this command to configure the policy action that terminates the policy script and sets the exiting status . The **no** form of this command deletes the action with the specified label.

action *label* **exit** [*result*]

no action *label*

Parameter description

Parameter	Description
label	Label of the action.
result	(optional) returned value of the Exit, it is 0 by default.

Default configuration

By default, 0 is returned when the policy is executed to the end.

Command mode

SEM configuration mode

Usage Guideline

In the synchronization mode, the operation of triggering the policy will wait for the completion of policy execution. And the returned value of the policy will determine whether to continue executing. If 0 is returned, stop running, while other values continue running.

The returned value of the policy is specified by the action exit and it is 0 by default.

Examples

The following example monitors the command line using the synchronization mode, when user inputs the “write memory” yes, it will prohibit the user operation and prompt the user.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_cli cli pattern "write memory" sync yes
Ruijie(config-applet)#action 00 puts "can not do this"
Ruijie(config-applet)#action 10 exit 0
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

The following example monitors the command line using synchronization mode, when user inputs the “line” yes, the aaa new-model is executed before the execution of the user command.

```
Ruijie(config)#smart manager applet Test_2
Ruijie(config-applet)#event tag monitor_cli cli pattern "line" sync yes
Ruijie(config-applet)#action 00 cli command "enable"
Ruijie(config-applet)#action 10 cli command "aaa new-model"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

action publish-event

In SEM configuration mode, use this command to configure the policy action that executes the Application Event sending. The **no** form of this command deletes the action with the specified label.

action *label* **publish-event sub-system** *sub-system-id* **type** *event-type* [**arg1** *argument-data*] [**arg2** *argument-data*] [**arg3** *argument-data*] [**arg4** *argument-data*]

no action *label*

Parameter description

Parameter	Description
label	Label of the action.
sub-system *sub-system-id*	Subsystem of the published event.
type *event-type*	Subtype of the published event.
arg1 *argument-data*	(optional) parametr1 of the event.
arg2 *argument-data*	(optional) parametr2 of the event.
arg3 *argument-data*	(optional) parametr3 of the event.
arg4 *argument-data*	(optional) parametr4 of the event.

Default configuration

By default, no action is configured.

Command mode

SEM configuration mode

Usage Guideline

This configuration is used with the event application. When the policy running the action publish-event has generated the message, the event application with the same sub-system and type will be triggered.

Examples

The following example monitors the event published by the action publish-event with the sub-system ID being 100 and type ID being 50, record logs after being triggered.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_event none
Ruijie(config-applet)#action 00 publish-event sub-system 100 type
50 arg1 para_1
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.
event application	

action reload

Use this command to reload the device in SEM configuration mode. The **no** form of this command deletes the action with the specified label.

action *label* **reload**

no action *label*

Parameter description

Parameter	Description
label	Label of the action.

Default configuration

By default, no action is configured.

Command mode

SEM configuration mode

Usage Guideline

N/A

Examples

The following example sets to reload the device when the memory of entire device is less than 20M.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_memory sysmon memory scope
system-free entry-op lt entry-val 20000
Ruijie(config-applet)#action 00 reload
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related

Command	Description

commands		
	smart manager applet	Define the command line based SEM policy.

action set

Use this command to set the local variable of policy in SEM configuration mode. The **no** form of this command deletes the action with the specified label.

action *label* **set** *variable-name variable-value*

no action *label*

Parameter description

Parameter	Description
label	Label of the action.
variable-name	Name of the local variable.
variable-value	Value of the local variable.

Default configuration

By default, no action is configured.

Command mode

SEM configuration mode

Usage Guideline

The local variable configured could have the same name with the global variable. When a local variable having the same name as the global variable is configured, the local variable will be used when such name is referred.

Examples

The following example sets the variable in the policy with none event type and sends the variable into the log.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag none_event none
Ruijie(config-applet)#action 00 set var_for_test "Test_1 running"
Ruijie(config-applet)#action 10 syslog msg "$var_for_test"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related

Command	Description

commands		
	smart manager applet	Define the SEM policy based on the command line.

action switchover

In SEM configuration mode, use this command to configure the policy action that executes the main/standby switchover forcibly. The **no** form of this command deletes the action with the specified label.

action *label* **switchover**

no action *label*

Parameter description

Parameter	Description
label	Labe of the action.

Default configuration

By default, no action is configured.

Command mode

SEM configuration mode

Usage Guideline

Current main/standby environmnet of the device is the prerequisite of executing the action. If the standby board is not ready, the policy execution will fail and be terminated.

Examples

The main/standby switchover will be executed forcibly if the "memory fail" occurs in the monitoring logs.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_log syslog pattern "memory fail"
Ruijie(config-applet)#action 00 switchover
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

action syslog

Use this command to configure the policy action that records logs in SEM configuration mode. The **no** form of this command deletes the action with the specified label..

action *label* **syslog** [**priority** *priority-level*] **msg** *msg-text* [**facility** *string*]

no action *label* **syslog**

Parameter description

Parameter	Description
label	Label of the action.
priority *priority-level*	(optional) set the level of logs.
msg *msg-text*	Content of logs.
facility *string*	Mnemonic symbol of logs.

Default configuration

By default, no action is configured.

Command mode

SEM configuration mode

Usage Guideline

N/A

Examples

The following example records logs when the CPU untilization of the entire device exceeds 95%.

```
Ruijie(config)#smart manager applet Test_2
Ruijie(config-applet)#event tag monitor_cpu sysmon cpu scope system
entry-op gt entry-val 95
Ruijie(config-applet)#action 00 syslog msg "system busy !"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

action wait

Use this command to configure the policy action that holds the policy script in SEM configuration mode. The **no** form of this command deletes the action with the specified label .

action *label* **wait** *wait-seconds*

no action *label* **wati**

Parameter description

Parameter	Description
label	Label of the action
wait-seconds	Length of time to wait.

Default configuration

By default, no action is configured..

Command mode

SEM configuration mode

Usage Guideline

N/A

Examples

Before executing the **show arp** command, execute the **clear arp-cache** and wait for 5 seconds.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_cli cli pattern "show arp"
sync yes
Ruijie(config-applet)#action 00 cli command "enable"
Ruijie(config-applet)#action 10 wait 5
Ruijie(config-applet)#action 20 exit 1
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy based on the.

commit

Use this command to submit current policy configurations in SEM configuration mode.

commit

Parameter description

Parameter	Description
-	-

Default configuration

By default, the policy configuration is not submitted.

Command mode

SEM configuration mode

Usage Guideline

N/A

Examples

The following example submits the policy configurations：

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag none-event none
Ruijie(config-applet)#action 00 set var_for_test "Test_1 running"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
rollback	Roll back the policy configurations.

Platform description

N/A

description

In SEM configuration mode, use this command to confiure the description of SEM policy. The **no** form of this command clears the description of SEM policy.

description *string*

no description

Parameter description

Parameter	Description
string	Text information for users to describe the SEM policy.

Default configuration

By default, no description of SEM policy is configured.

Command mode

SEM configuration mode

Usage Guideline

The change to the pocily description takes effect immediately without the need to submit.

Examples

The following example sets the description of current SEM policy to “Descrption_For_SEM_Applet”

```
Ruijie(config-applet)#description Descrption_For_SEM_Applet
```

The following example clears the description of current SEM policy.

```
Ruijie(config-applet)#no description
```

Related commands

Command	Description
smart manager applet	Define the SEM policy based on the command line.

event application

In SEM configuration mode, this command monitors the event published by the action publish-event. The **no** form of this command is used to delete the specified event.

event tag *event-name* [**correlate** {**andnot** | **and** | **or** }] **application subsystem** *subsystem-id* **type** *event-type*
no event tag *event-name*

Parameter description

Parameter	Description
event-name	Event name.
correlate {andnot | and |or}	(optional) correlationship between current event and previous all event combinations in the case of multiple events.
subsystem	Subsystem ID of the monitored event.

subsystem-id	
type *event-type*	Type ID of the minotored event.

Default configuration

By default, no event is configured.

Command mode

SEM configuration mode

Usage Guideline

The **event application** command is used to monitor the events published by **action publish-event to allow one policy to drive another**.

subsystem-id and **event-type** are used to differentiate events. A policy is triggered only when the **subsystem-id** and **event-type** published by **action publish-event** are identical with those set by this command.

Available events:

Variable Name	Function
_application_sub_system	Indicates the subsystem that publishes a certain event
_application_type	Indicates the type of the published event
_application_data1	Indicates parameter 1 for event publishing
_application_data2	Indicates parameter 2 for event publishing
_application_data3	Indicates parameter 3 for event publishing
_application_data4	Indicates parameter 4 for event publishing

Examples

The following example monitors the event published by the action publish-event with the demand of subsystem ID being 100, type ID being 50 and recording logs after triggering

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_event application
sub-system 100 type 50
Ruijie(config-applet)#action 00 syslog msg "Have event :subsystem
$_application_sub_system type $_application_type"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command lined based SEM policy.
action publish-event	Publish the action of application event.

event cli

In SEM configuration mode, use this command to confiure command line monitoring. The **no** form of this command deletes the event of specified name.

event tag event-name [**correlate** {**andnot** | **and** |**or**}] **cli pattern** *regular-expression* [**sync** {**yes** [**default** *wait-time*] | **no skip** {**yes** | **no**}}] [**mode** *variable*] [**occurs** *num-occurrences*] [**period** *period-value*]

no ip msdp mesh-group *mesh-name peer-address*

Parameter description

Parameter	Description
event-name	Event name.
correlate {andnot | and |or}	(Optional) in the case of multiple events, the correlationship between current event and previous all event combinations
pattern *regular-expression*	The character string matched to the user command line mode.
sync{ **yes | no**}	(Optional) it determines whether to execute the policy synchronously.
skip { **yes | no** }	(Optional) it determines whether to skip this command, this function is used only in the asynchronous condition and it is no by default.
default *wait-time*	(Optional) maximum time of command line waiting for the end of policy running, it is used on condition that the command line synchronizes with policy. 30 seconds by default.
mode *variable*	(Optional) match the command mode, all modes are matched by default.
occurs *num-occurrences*	(Optional) the matching times which is needed for triggering Event. It is 1 by default.
period *period-value*	(Optional) invalid period of **occurs** command, the duration of occurs operation over the

	period-value will be considered as time-out. This parameter is invalid when the **occurs** is 1.

Default configuration

By default, no event is configured.

Command mode

SEM configuration mode

Usage Guideline

The reference command used to pattern commands is a command line, instead of the short form. For example, to **pattern *write memory, you an enter write memory or write mem.***

When option sync is set to **yes**, the command line does not respond until the policy execution completes. If the returned value is not **0**, the command will be executed normally. If the returned value is **0**, the command will not be executed.

When option sync is set to **no**, option **skip** is available. If you set **skip** to **no**, the command will be executed normally. If you set **skip** to **yes**, the command will not be executed.

Option **mode specified the command patterning mode. If you use a different mode while entering the command,** patterning is performed.

Option **default** specifies the timeout when the command line will wait for the completion of policy execution. Therefore, this option takes effect only when **sync** is set to **yes**.

Option **occurs** specifies the occurrence times of an event for triggering the policy. When the event occurs for the times specified by ***num-occurrences* within a certain period, the policy will be triggered.**

Option period specifies the timeout period of option **occurs**.

Caution: The policy configuration command line you enter may also be patterned. If **skip** is **yes**, or **sync** is **yes** and the returned value of the policy is **0**, the command will not be executed.

For key commands such as **enable**, setting **skip** to **yes**, or setting **sync** to **yes** and policy return value being **0** may render the commands invalid.

Available events:

Variable Name	Function
_cli_msg	Indicates the content of the entered command line
_cli_msg_count	Indicates the length of the entered command line
_cli_mode	Indicates the command mode

Examples

The following example monitors the command line input with recording logs when users input the **show ip route** command.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_input cli pattern "show ip
route" sync no skip no
Ruijie(config-applet)#action 00 syslog msg "show ip route running"
Ruijie(config-applet)#action 10 exit 1
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

The following example monitors the command line input with preventing the user from inputing the **shutdown** command in the interface configuration mode.

```
Ruijie(config)#smart manager applet Test_2
Ruijie(config-applet)#event   tag   monitor_input   cli   pattern
"shutdown" mode interface
Ruijie(config-applet)#action 00 puts "can not do this"
Ruijie(config-applet)#action 10 exit 0
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

event counter

In SEM configuration mode, this command monitors the SEM counter. The **no** form of this command deletes the event of specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **counter name** *counter-name* **entry-op** *operator* **entry-val** *entry-value* **exit-op** *operator* **exit-val** *exit-value*

no event tag *event-name*

Parameter description

Parameter	Description
event-name	Event name.
correlate {andnot | and | or}	(Optional) correlationship between current event and previous all event combinations in the case of multiple events.
name *counter-name*	Specify the name of the counter monitored.
entry-op *operator*	The method that triggers comparision: eq equal to ge greater than or equal to gt greater than le less than or equal to lt less than ne unequal to
entry-val *entry-value*	The value that triggers comparison
exit-op *operator*	The method that recovers comparision: eq equal to ge greater than or equal to gt greater than le less than or equal to lt less than ne unequal to
exit-val *exit-value*	The value that recover comparison.

Default configuration

By default, no event is configued.

Command mode

SEM configuration mode.

Usage Guideline

The **event counter** command is used to monitor the named counters in SEM, which are usually changed by the action counter.

When the combinations between the command counter and **entry-op**/**entry-val** are patterned successfully, an event is triggered. Then, the current patterning stops, meaning the event detection fails.

When triggered patterning stops, the combinations between the command counter and **exit-op**/**exit-val** are patterned. If the patterning succeeds, the combined patterning with **entry-op** and **entry-val** recovers.

Available events:

Variable Name	Function
_counter_name	Indicates the name of the named counter
_counter_value	Indicates the value of the named counter

Examples

The following example configures policy counter **Test_Counter**. When the value of **Test_Counter** is larger than 10, a log is generated and **Test_Counter** is set to **0**. When the value of **Test_Counter** is larger than 5, monitoring recovers.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_counter counter name
Test_Counter entry-op ge entry-val 10 exit-op gt exit-val 5
Ruijie(config-applet)#action 10 counter name Test_Counter op set
value 0
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.
action counter	

event cpp

This command is used to configure a CPP-based event in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **cpp parameter** {*counter-name* | **any**} **type** {**pps** | **total** | **drop**} **op** *operator* **value** *value* [**slot** { *slotid* | **mboard** }] **poll-interval** *poll-int-value*

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The

	values are **and**, **or**, and **andnot**.
parameter {*counter-name* | **any**}	The packet type
type {**pps** | **total** | **drop**}	The packet statistics type
op *operator*	The comparing method: **eq**: equal to **ge**: greater than or equal to **gt**: greater than **le**: less than or equal to **lt**: less than **ne**: unequal to
value *value*	The comparison value
slot { *slotid* | **mboard** }	The monitored board, the mboard means the management board.
poll-interval *poll-int-value*	The poll interval.

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

Available events:

Variable Name	Function
_cpp_slot	Monitored slot
_cpp_parameter	Packet type
_cpp_type	Packet statistics type
_cpp_value	Actual value

Examples

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)# event tag event_1 cpp parameter any type drop
op ge value 1000 poll-interval 15
```

```
Ruijie(config-applet)# action action_1 cli command "enable"
Ruijie(config-applet)# action action_2 cli command "configure
terminal"
Ruijie(config-applet)# action action_3 cli command "cpu-protect
type $_type pri 0"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

Platform description

N/A

event grtd

This command is used to configure a GRTD-based event in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **grtd slot** {*slot-num* | **all** | **master** | **slave** } [**testing-type** {**bootup** | **ondemand** | **schedule** | **monitoring**}] [**test-name** *test-name*] [**test-id** *test-id*] [**severity-major**] [**severity-minor**] [**severity-normal**]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
slot {*slot-num* | **all** | **mboard** | **slave** }	The monitored slot
testing-type {**bootup** | **ondemand** | **schedule** | **monitoring**}	Monitoring type: **bootup** for bootup test, **ondemand** for command test, **schedule** for schedule test, and **monitoring** for monitoring test
test-name *test-name*	The test name
test-id *test-id*	The test ID

[severity-major] [severity-minor] [severity-normal]	Indicate the fault level: **severity-major** for major faults, **severity-normal** for normal faults, and **severity-minor** for minor faults

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

Available events:

Variable Name	Function
_grtd_test_slot	Board that trigger an event
_grtd_test_type	Event type
_grtd_test_name	Test name
_grtd _test_id	Test ID
_grtd _test_severity	Fault level

Examples

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_grtd grtd slot all
severity-major severity-normal
Ruijie(config-applet)#action 00 syslog msg "grtd detect some
failure"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

Platform description

N/A

event interface

In SEM configuration mode, use this command to configure statistics on the monitoring interface of a monitor. Use the **no** form of this command to delete the event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **interface name** *interface-type interface-number* **parameter** *counter-name* **entry-op** *operator* **entry-val** *entry-value* **entry-type** {**value** | **increment** | **rate**} **poll-interval** *poll-int-value* [**exit-op** *operator* **exit-val** *exit-value* **exit-type** {**value** | **increment** | **rate**} [**exit-comb** {**or** | **and**}] [**exit-time** *exit-time-value*]] [**average-factor** *average-factor-value*]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
name *interface-type interface-number*	The interface name.
parameter *counter-name*	The statistics type of the monitoring interface.
entry-op *operator*	The method that triggers comparison: **eq**: equal to **ge**: greater than or equal to **gt**: greater than **le**: less than or equal to **lt**: less than **ne**: unequal to
entry-val *entry-value*	The value that triggers comparison.
entry-type {**value** | **increment** | **rate**}	The value type that triggers comparison.
poll-interval *poll-int-value*	Comparing interval. By default, it is 5s.
exit-comb {**or** | **and**}	The relation between **exit-op** and **exit-time.**
exit-op *operator*	The method to recover comparison (optional): **eq**: equal to **ge**: greater than or equal to **gt**: greater than **le**: less than or equal to

	lt: less than **ne**: unequal to
exit-val *exit-value*	The value to recover comparison (optional).
exit-type {**value** | **increment** | **rate**}	The value type to recover comparison (optional).
exit-time *exit-time-value*	The minimum time between triggering and monitoring recovery (optional).
average-factor *average-factor-value*	It is used by **rate**, and is the changed statistical period when multiplied by *poll-int-value.*

Default configuration

No event is configured.

Command mode

SEM configuration mode.

Usage Guideline

The **parameter** of **event interface** includes the following parameters:

■	input_errors	Number of damaged packets received
■	input_errors_crc	Number of packets received with CRC errors
■	input_errors_frame	Number of framing ERR packets received
■	input_errors_overrun	Number of overruns and resource errors
■	input_packets_dropped	Number of packets dropped from input Q
■	interface_resets	Number of times an interface has been reset
■	output_buffer_failures	Number of failed buffers
■	output_buffer_swappedout	Number of packets swapped to DRAM
■	output_errors	Number of packets errored on output
■	output_errors_underrun	Number of underruns on output
■	output_packets_dropped	Number of packets dropped from output Q
■	receive_broadcasts	Number of broadcast packets received
■	receive_giants	Number of too large packets received
■	receive_rate_bps	Interface receive rate in bits/sec
■	receive_rate_pps	Interface receive rate in pkts/sec

■ receive_runts	Number of too small packets received
■ receive_throttle	Number of times the receiver was disabled
■ reliability	Interface reliability as a fraction of 255
■ rxload	Receive rate as a fraction of 255
■ transmit_rate_bps	Interface transmit rate in bits/sec
■ transmit_rate_pps	Interface transmit rate in pkts/sec
■ txload	Transmit rate as a fraction of 255

Available events:

Variable Name	Function
_interface_is_increment	Indicates the detector mote of the interface
_interface_name	Indicates the interface name
_interface_parameter	Indicates the parameter type of the detection interface
_interface_value	Indicates the interface count

Examples

The following example configures to perform detection every 5 s. If **interface_resets** of GigabitEthernet3/0 creases, a log is generated.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config)#event tag monitor_interface interface name GigabitEthernet3/0 parameter interface_resets entry-op ge entry-val 1 entry-type increment exit-op eq exit-val 1 exit-type increment poll-interval 5
Ruijie(config-applet)#action 00 syslog msg "$_interface_name reseted"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
intelligence manager applet	Define the command line based SEM policy.
show interfaces	View the interface information

Platform description

N/A

Platform description

N/A

event none

In SEM configuration mode, this command is used to configure a monitor of the **smart manager run** command. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or** }] **none** [**sync** {**yes** [**default** *wait-time*]| **no**}]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
sync {**yes** | **no**}	Indicate whether to execute the policy synchronously, that is, execute the command after policy execution completes (optional). By default, the policy is executed synchronously.
default *wait-time*	Indicate the timeout when the command line will wait for the completion of policy execution (optional). The default value is 30s.

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

This command is used to configure a monitor of the entered **intelligence manager run** command. It is the policy that triggers manual command execution and is used to execute scripts in batches.

Available events:

Variable Name	Function
_policy_name	Policy name
_none_argc	Number of parameters
_none_arg1	Parameter 1
_none_arg2	Parameter 2

_none_arg3	Parameter 3
_none_arg4	Parameter 4
_none_arg5	Parameter 5

Examples

The following example configures a **none** type event with the name as **Test_1**. When this event is triggered, a log is generated.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_cmd none
Ruijie(config-applet)#action 00 syslog msg "none event triggered
with $_none_argc argc"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
intelligence manager applet	Define the command line based SEM policy.
intelligence manager run	Run the **none** event.

Platform description

N/A

event oir

This command is used to configure a monitor of hot-swap events in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **oir** [**type** {**plugin** | **remove**}] [**slot** {*slot-num* | **slave**}]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**
type {**plugin** | **remove**}	The monitored plug-in and removal events (optional)
slot {*slot-num* |	The monitored slot No. (optional), the slave

slave}	means the slave management board.

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

Available events:

Variable Name	Function
_oir_event	plug-in and removal
_oir_slot	Slot No.

Examples

The following example configures a monitor of board plug-in or removal to or from the device. When a board is plugged in or removed, a log is generated.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_oir oir
Ruijie(config-applet)#action 00 syslog msg "plugin or remove
$_oir_event $_oir_slot"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

The following example configures the monitored slot as **1**. When the board in slot 1 is removed, a log is generated.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event monitor_oir oir type remove slot 1
Ruijie(config-applet)#action 00 syslog msg "Slot $_oir_slot hot
removed"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

event snmp

This command is used to configure a monitor of SNMP objects in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **snmp oid** *oid-value* **get-type** {**exact** | **next**} **entry-op** *operator* **entry-val** *entry-value* **entry-type** {**value** | **increment** | **rate**} **poll-interval** *poll-int-value* [**exit-op** *operator* **exit-val** *exit-value* **exit-type** {**value** | **increment** | **rate**} [**exit-comb** {**or** | **and**} **exit-time** *exit-time-value*]] [**average-factor** *average-factor-value*]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
oid *oid-value*	The monitored SNMP OID
get-type {**exact** | **next**}	The SNMP operation mode, including direct operation and get next.
entry-op *operator*	The method that triggers comparison: **eq**: equal to **ge**: greater than or equal to **gt**: greater than **le**: less than or equal to **lt**: less than **ne**: unequal to
entry-val *entry-value*	The value that triggers comparison.
entry-type {**value** | **increment** | **rate**}	The value type that triggers comparison.
exit-comb {**or** | **and**}	The relation between **exit-op** and **exit-time.**
exit-op *operator*	The method to recover comparison (optional): **eq**: equal to **ge**: greater than or equal to **gt**: greater than **le**: less than or equal to **lt**: less than **ne**: unequal to
exit-val *exit-value*	The value to recover comparison (optional)

exit-type {**value** | **increment** | **rate**}	The value type to recover comparison (optional).
exit-time *exit-time-value*	The minimum time between triggering the policy and monitoring recovery (optional).
average-factor *average-factor-value*	It is used by **rate**, and is the changed statistical period when multiplied by *poll-int-value*
poll-interval *poll-int-value*	The comparing interval. By default, it is 5s.

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

Available events:

Variable Name	Function
_snmp_oid	SNMP OID
_snmp_oid_delta_val	Difference between the actual SNMP OID value and the set value
_snmp_oid_val	Actual SNMP OID value

Examples

The following example configures to monitor snmp oid 1.3.6.1.2.1.2.2.1.10.1. If the value is larger than 10000, a log is generated.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_snmp snmp oid 1.3.6.1.2.1.2.2.1.10.1 get-type exact entry-op ge entry-val "10000" entry-type value poll-interval 5
Ruijie(config-applet)#action 00 syslog msg "$_snmp_oid out of range"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

Platform description N/A

event snmp-notification

This command is used to configure a monitor of SNMP Traps in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **snmp-notification oid** *oid-string* **oid-val** *comparison-value* **op** *operator* [**skip** {**yes** | **no**}]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
oid *oid-string*	The monitored OID
oid-val *comparison-value*	The reference value for monitoring
op *operator*	The comparing method
skip {**yes** | **no**}	Indicate whether to skip the snmp trap. If it is set to yes, the patterned snmp trap will be skipped. The default setting is no.

Default configuration No event is configured.

Command mode SEM configuration mode

Usage Guideline

Available events:

Variable Name	Function
_snmp_notif_oid	Trap OID
_snmp_notif_oid_val	Trap OID value

Examples

The following example configures to monitor the Trap message with the OID as **1.3.6.1.2.1.52.2.1** sent by the device. When the OID value of the Trap message is larger than 1000, the policy is triggered.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_trap snmp-notification oid 1.3.6.1.2.1.52.2.1 op gt oid-val 1000
Ruijie(config-applet)#action 00 syslog msg "have trap $_snmp_notif_oid value $_snmp_notif_oid_val"
Ruijie(config-applet)#action 10 exit 1
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

Platform description

N/A

event snmp-object

This command is used to configure a monitor of the get, set, and get next operations on SNMP objects in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **snmp-object [operate {get|getnext|set}] oid** *oid-value* **type** *value* **istable** {**yes** | **no**} **skip** {**yes** | **no**}

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
operate {get|getnext|set}	(Optional) SNMP operation type.
oid *oid-value*	The monitored SNMP OID.
type *value*	The monitored OID type.
istable {**yes** | **no**}	Indicate whether SNMP OID is a table.
skip {**yes** | **no**}	(Optional) indicate whether to skip the SNMP operation, the default setting is no.

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

Available events:

Variable Name	Function
_snmp_oid	SNMP OID
_snmp_request_type	SNMP request type
_snmp_value	SNMP request value

Examples

The following example configures to monitor the modification of SNMP OID **1.3.6.1.2.1.1.4**. When it is modified, a log is generated.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor-snmpobj snmp-object oid
1.3.6.1.2.1.1.4 type octet sync yes
Ruijie(config-applet)#action 00 syslog msg "_snmp_oid : $_snmp_oid
_snmp_request_type : $_snmp_request_type _snmp_value :
$_snmp_value"
Ruijie(config-applet)#action 10 exit 1
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

Platform description

N/A

event syslog

This command is used to configure a log monitor in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **syslog pattern** *regular-expression* [**priority** *priority-level*] [**occurs** *num-occurrences*] [**period** *period-value*] [**skip** {**yes** | **no**}]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
pattern *regular-expression*	The character string for log content patterning.
priority *priority-level*	Pattern the log priority.
occurs *num-occurrences*	The occurrence times to trigger an event (optional). By default, it is 1.
period *period-value*	The validity period of the **occurs** operation (optional). When the time set by ***period-value*** is due, the **occurs** operation times out. This parameter is invalid when **occurs** is **1**.
skip {**yes** | **no**}	Indicate whether to skip the Syslog. If it is set to yes, the patterned log will be skipped. The default setting is no.

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

Available events:

Variable Name	Function
_syslog_msg	Syslog message
_priority	Syslog priority

Examples

The following example configures to monitor logs. When the string "memory fail" is detected, active/standby switchover will be forced.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_log syslog pattern "memory fail"
Ruijie(config-applet)#action 00 force-switchover
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

Platform description

N/A

event sysmon

This command is used to configure a system resource monitor in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or** }] **sysmon type** {**cpu** {**system** | **task** task-name } | **memory** {**system-use** | **system-free** | **task** task-name} {**percent** | **absolute**}} **entry-op** *operator* **entry-val** *entry-value* **poll-interval** *poll-int-value* [**exit-op** *operator* **exit-val** *exit-value*] [**slot** { *slot-num* | **slave** [**subsystem** *subsystem-id*]}]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
cpu {**system** | **task** task-name}	Monitor the CPU ultization by the system or a certain task.
memory {**system-use** | **system-free** | **task** task-name }	Monitor the memory utilization and free memory of the system or a certain task
entry-op *operator*	The method that triggers comparison: **eq**: equal to **ge**: greater than or equal to **gt**: greater than **le**: less than or equal to **lt**: less than **ne**: unequal to
entry-val *entry-value*	The value that triggers comparison.
poll-interval *poll-int-value*	The comparing interval. By default, it is 5s.

exit-op *operator*	The method to recover comparison (optional): **eq**: equal to **ge**: greater than or equal to **gt**: greater than **le**: less than or equal to **lt**: less than **ne**: unequal to
exit-val *exit-value*	The value to recover comparison (optional)
slot { *slot-num* | **slave** }	The detected slot, the salve means the slave management board.
subsystem *subsystem-id*	The detected subsystem, which is used for the multiple CPU board (optional).

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

The **event system** command is used to monitor the following items:

CPU utilization by the system: **type cpu scope system**

CPU utilization by a certain task: **type cpu scope task task-name**

Memory utilization by the system: **type memory scope system-use percent**

Absolute memory utilization by the system: **type memory scope system-use absolute**

Free memory of the system: **type memory scope system-free percent**

Absolute free memory of the system: **type memory scope system-free absolute**

Memory utilization by a certain task: **type memory scope task task-name percent**

Absolute memory utilization by a certain task: **type memory scope task task-name absolute**

Available events:

Variable Name	Function
_mon_type	Indicates the detection type
_value	Indicates the monitored value

Examples

The following example configures to restart the device when the free memory is less than 20M.

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_memory sysmon memory scope system-free entry-op lt entry-val 20000
Ruijie(config-applet)#action 00 reload
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

The following example configures to generate a log when the system CPU utilization exceeds 95%.

```
Ruijie(config)#intelligence manager applet Test_2
Ruijie(config-applet)#event monitor_cpu sysmon cpu scope system entry-op gt entry-val 95
Ruijie(config-applet)#action 00 syslog msg "system busy !"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

event timer

This command is used to configure a time-based event in SEM configuration mode. The **no** form of this command is used to delete an event with the specified name.

event tag *event-name* [**correlate** {**andnot** | **and** | **or**}] **timer** {**absolute** {**unix** *time-value* | **date** date-value} | **countdown time** *time-value* | **cron cron-entry** *cron-entry* | **watchdog time** *time-value*} [**name** *timer-name*]

no event tag *event-name*

Parameter description

Parameter	Description
event-name	The event name.
correlate { **andnot** | **and** | **or** }	The relation between the current event and the combination of the previous events in the case of multiple events (optional). The values are **and**, **or**, and **andnot**.
absolute unix *time-value*	Use the UNIX-format date and time to trigger an event.
absolute date date-value	Use the Date-format date and time to trigger an event.
countdown time *time-value*	Use a timer to trigger an event.

cron cron-entry *cron-entry*	Use the Cron configuration to trigger an event.
watchdog time *time-value*	Use the cycling timer time to trigger an event.
name *timer-name*	Specify the timer name (optional)

Default configuration

No event is configured.

Command mode

SEM configuration mode

Usage Guideline

Time-based events can be divided into the following four classes:

- A specific data and time
- A time point when the configuration takes effect
- Time described by the Cron format
- Trigger by the cycling timer

The time in “a specific data and time” can be in Date time or Unix-format time.

Available events:

Variable Name	Function
_timer_type	Timer type

Examples

Example 1: Restart the device at Unix-format time **1257831095** .

```
Ruijie(config)#intelligence manager applet Test_1
Ruijie(config-applet)#event tag monitor_timer timer absolute time
1257831095
Ruijie(config-applet)#action 00 reload
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Example 2: Send log “3600 second arrival” after 3600s.

```
Ruijie(config)#intelligence manager applet Test_2
Ruijie(config-applet)#event tag monitor_timer timer countdown time
3600
Ruijie(config-applet)#action 00 syslog msg "3600 second arrival"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Example 3: Clear the ARP buffer every 7200.

```
Ruijie(config)#intelligence manager applet Test_3
Ruijie(config-applet)#event tag monitor_timer timer watchdog time
7200
Ruijie(config-applet)#action 00 cli command "enable"
Ruijie(config-applet)#action 10 cli command "clear arp-cache"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Example 4: Clear route at 0 o’clock everyday.

```
Ruijie(config)#intelligence manager applet Test_4
Ruijie(config-applet)#event tag monitor_timer timer cron cron-entry
"0 0 * * *"
Ruijie(config-applet)#action 00 cli command "enable"
Ruijie(config-applet)#action 10 cli command "clear ip route *"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

Platform description

N/A

list-config

Use this command to show currrent policy configurations in SEM configuration mode.

list-config

Parameter description

Parameter	Description
-	-

Default configuration

None

Command mode

SEM configuration mode

Usage Guideline N/A

Examples N/A

Related commands

Command	Description
commit	Submit the policy configurations.
rollback	Roll back the policy configuratioins.

policy record

In SEM configuration mode, configure to record CLI action outputs and configure the size of CLI action outputs.

policy record [**per-instance** *record-size-per-policy*] [**per-policy** *record-size-per-policy*]

no policy record

Parameter description

Parameter	Description
per-instance *record-size-per-policy*	(Optional) size of CLI records when the policy is triggered each time; unit: kbytes; default: 50
per-policy *record-size-per-policy*	(Optional) gross size of all CLI records triggered by the policy; unit: kbytes; default: 1000

Default configuration CLI action outputs are not recorded by default.

Command mode SEM configuration mode

Usage Guideline By default, the outputs of CLI action executed by the SEM policy are not recorded. After configuring policy record, when CLI action is executed, outputs of CLI action will be recorded into the file system. The path of log file is: "/sem_record/policy_name/yyyy-mm-dd_hh-mm-ss_mspolicytriggerid.txt". Therein, "/sem_record/" is the general directory for the output records of all CLI actions, and is located in the root directory of file system; "policy_name" is the name of policy, and is located in the directory of

"/sem_record/"; each policy corresponds to each separate directory. "yyyy-mm-dd_hh-mm-ss_mspolicytriggerid.txt" is the name of log file, and is the combination of date and time when this record is generated and the policy trigger ID.

Use **more** command to view logs.

When the number of CLI action outputs exceeds the size configured with the parameter of per-instance record-size-per-policy, the earliest records will be overwritten.

When the gross size of the log file of CLI action outputs generated during the running of a specific policy exceeds the value set in per-policy record-size-per-policy, the earliest logs will be cleared until the total size of log file complies with the value set in per-policy record-size-per-policy.

Execute **smart manager policy record clean** command to clear CLI action output records in the file system.

Examples

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag none-event none
Ruijie(config-applet)#action 00 cli command "enable"
Ruijie(config-applet)#action 10 cli command "show arp"
Ruijie(config-applet)#policy record
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
Ruijie(config)# exit
Ruijie# more /sem_record/Test_1/2010-01-01_01-00-00_1001.txt
                    SEM CLI RECORD FILE
SEM policy name: Test_1
SEM policy trigger id :1
SEM policy cli record time : Fri Jan 01 01:00:00 2010
==================================================
Ruijie#enable
Ruijie#show arp
Protocol  Address     Age(min)  Hardware       Type   Interface
Internet  6.6.6.6        21    0027.1994.e59b  arpa   VLAN 1
Internet  6.6.6.1        --    00d0.f822.33b3  arpa   VLAN 1
Total number of ARP entries: 2
Ruijie#
```

Related commands

Command	Description
action cli	Execute CLI commands.

smart manager policy record	Clear CLI records generated during the execution of the SEM policy.

rollback

Use this command to roll back current policy configurations in SEM configuration mode.

rollback

Parameter description

Parameter	Description
-	-

Default configuration

By default, the policy configuration is not rolled back.

Command mode

SEM configuration mode

Usage Guideline

N/A

Examples

The following example rolls back the policy configurations:

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag none-event none
Ruijie(config-applet)#action 00 set var_for_test "Test_1 running"
Ruijie(config-applet)#rollback
Ruijie(config-applet)#exit
```

Related commands

Command	Description
commit	Submit the policy configurations.

smart manager applet

In the global configuration mode, use this command to define a SEM policy. The **no** form of this is used to delete a SEM policy.

smart manager applet *applet-name* [**class** *class-options*]
no smart manager applet ***applet-name*** **[**reserve-record **|**clean-record**]**

Parameter description

Parameter	Description
applet-name	Define the name of the SEM policy, which should consist of numbers, letters and underline.
class *class-options*	(optional) Specify the class of the policy . The default class is **default**..
reserve-record	Reserve the CLI record file generated by policy execution.
clean-record	Delete the CLI record file generated by policy execution.

Default configuration

By default, the policy based on the command line is not configured.

Command mode

Global configuration mode

Usage guidelines

A policy can include the following configurations:

- One or more events
- One or more actions
- Policy description (optional)
- Policy triggering information (optional)

Running the **smart manager applet** command enters the SEM configuration mode. In this mode, you can complete the following operations:

- Configuring an event for the policy
- Configuring an action for the policy
- Configuring the description of the policy
- Configuring the triggering parameter of the policy
- Submitting the policy configuration
- Rolling back the policy configuration
- Viewing the current policy configuration

Each event must have a unique name specified by parameter **tag**. SEM automatically arranges events by tag alphabetically. Each action must be assigned a unique label. SEM automatically arranges actions by label alphabetically. When a policy is activated, actions are performed by label alphabetically.

In SEM configuration mode, you can use environment variables in policy actions. There are two kinds of variables:

- Global variable
- Local variable

A local variable can be defined by a system event detector when an event occurs, or by an action while a policy is running. For the system variables that are generated by each kind of event, refer to use guide.

Note Each policy corresponds to a class. The default class is **default**. Multiple policies can belong to one class. A class is used to allocate thread resources to and specify the running priority for the policies in it.

Note The policy configuration does not take effect until the **commit** command is used in SEM configuration mode to submit it.

A policy is checked for validity when it is submitted. If the policy configuration does not pass the validity check, policy registration and the submission fail.

A policy without any event configured cannot pass the validity check.

A policy without action can pass the validity check, but does nothing after being triggered. Therefore, an alarm is sent when such a policy is submitted.

To give up your policy modification, you can use the **rollback** command to roll back.

Note The SEM policy does not take effect when starting up the device, and it takes effect only when the configuration configured on the device's Cosole is available. For details, refer to the **smart manager policy bootup-delay**.

Note When several events are configured for a policy, SEM automatically arranges the events alphabetically in a parallel relationship. The other events are taken as the additional conditions of the first event. The relations among all the events except the first event are the one between current event and the combination of all the previous events. Therefore, the first event is blocked out for the parallel relationship and the default relation is **and**.

Note When several events are configured for a policy, SEM automatically arranges the events alphabetically in a parallel relationship. The other events are taken as the additional conditions of the first event. The relations among all the events except the first event are the one between current event and the combination of all the previous events. Therefore, the first event is blocked out for the parallel relationship and the default relation is **and**.

Event variables available to all policies:

Variable Name	Function
_event_id	Indicates the event triggering ID
_event_type	Indicates the type ID of the event detector that triggers the policy
_event_type_string	Indicates the description of the event detector that triggers the policy
_event_pub_time	Indicates the start time of the event
_event_pub_sec	Indicates the start time of the event (UNIX time)
_event_pub_msec	Indicates the start time (in ms) of the event

Examples

Example 1: Create a command line based policy with the name as **Test_A**.

```
Ruijie(config)#smart manager applet Test_A
Ruijie(config-applet)#
```

Example 2: Create a command line based policy with the name as **Test_B** and class as **D**.

```
Ruijie(config)#smart manager applet Test_B class D
Ruijie(config-applet)#
```

Field	Description
class D	Groups the policy to class D

Related commands

Command	Description
smart manager policy bootup-delay	Set the bootup-delay of SEM policies.
show smart manager pocily registered	Show the registered policy.

smart manager environment

In the global configuration mode, use this command to define a SEM global variable. The no form of this command is used to delete the specified SEM global variable.

smart manager environment *variable-name string*

no smart manager environment *variable-name*

Parameter description

Parameter	Description
variable-name	Define the variable name.
string	Define the variable value.

Default configuration

By default, the SEM global variable is not defined.

Command mode

Global configuration mode

Usage guidelines

A variable is a string with its meaning depending on the specific scenario.

Global variables can be used in all policies. The system and users can define local variables with the same name. Global variables become invalid when being invoked by policies, while local variables take effect.

Examples

Example 1: Define a global variable with the name as **variable_name** and value as **variable_value**.

```
Ruijie(config)#smart    manager    environment    variable_name
variable_value
```

Related commands

Command	Description
show smart manager environment	Show the global environment variable.

smart manager history

In the global configuration mdoe, use this command to configure the maximun number of SEM history information to be saved. The **no** form of this command is used to restore it to the default value.

smart manager history size events *size*

no smart manager history size events

Parameter description

Parameter	Description
events	Set the maximum number of SEM history information to be saved.

sizes	Set the specified number, its the maximum value is 50 and default value is 50 also.

Default configuration

50.

Command mode

Global configuration mode

Usage Guideline

Caution

Try not to set the maximum value to 0. if so, the SEM will not record the histoty information.

Examples

The following example sets the maximum saved number of SEM Even history information to 30:

```
Ruijie(config)#smart manager history size events 30
```

Related commands

Command	Description
show smart manager history events	Show the event history information.

smart manager policy bootup-delay

In the global configuration mdoe, use this command to configure the bootup-delay of SEM policies.

smart manager policy bootup-delay *dealy-time*

Parameter description

Parameter	Description
delay-time	The interval ranges from the SEM policy is available in the console to the SEM policy is used, in the range of 60seconds-900seconds.

Default configuration

60 seconds.

Command mode

Global configuration mode

Usage Guideline

N/A

Examples

The following example sets the bootup-delay to 120 seconds:

```
Ruijie(config)#smart manager policy bootup-delay 120
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

smart manager policy record

In the privileged mdoe, use this command to clear the CLI record generated by running the SEM policy.

smart manager policy record clean [**no-registed** | **policy** *registed-polciy-name* | **dir** *record-directory* | **all**]

Parameter description

Parameter	Description
no-registed	Clear all CLI record directories of the policies that have not registered in the SEM system.
policy *registed-policy-name*	Clear the CLI record generated by the specified registered policy.
dir *record-directory*	Clear the specified CLI record directory in the SEM reocrd.
all	Clear all CLI record directories in the SEM reocrd.

Default configuration

N/A

Command mode

Privileged configuration mode

Usage Guideline

N/A

Examples

The following example clears all CLI ouput records of the unregistered policies:

```
Ruijie#smart manager policy record clean no-registed
```

The following example clears all CLI ouput records generated by running the SEM policy:

```
Ruijie#smart manager policy record clean all
```

Related commands

Command	Description
action cli	Execute the CLI.
policy record	Configure the ouput record which records the CLI action.

smart manager run

In the privileged EXEC mode, use this command to run the policy of the events with none type.

smart manager run *policy-name* [*parameter*]

Parameter description

Parameter	Description
policy-name	Policy name of the event with none type.
parameter	(optional) parameters of the excuted policy, up to five parameters can be configured.

Default configuration

By default, it is not executed.

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example configures the name of the event with none type to Test_1, and logs after triggered.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag monitor_cmd none
Ruijie(config-applet)#action 00 syslog msg "none event triggered
with $_none_argc argc"
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

smart manager scheduler clear

In the privileged EXEC mode, this command clears the SEM event queues.

smart manager scheduler clear {all | policy *job-id* **|class** *class-options* **}**

Parameter description

Parameter	Description
all	All policies
policy *job-id*	Specify the trigger ID of the policy.
class *class-options*	Specify the policy class

Default configuration

By default, no policy running instance is cleared.

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example clears all types of queues.

```
Ruijie#smart manager scheduler clear all
```

The following example clears all queues of policy with the type of applet and the Class B.

```
Ruijie#smart manager scheduler clear class B
```

Related

Command	Description

commands

smart manager applet	Define the command line based SEM policy.

Platform description

N/A

smart manager scheduler hold

In the privileged EXEC mode, this command holds the SEM scheduler.

smart manager scheduler hold { all | policy *job-id* **| class** *class-optionas* **}**

Parameter description

Parameter	Description
all	All policies.
job *job-id*	Specify the trigger ID of the policy.
class *class-options*	Specify the policy class.

Default configuration

By default, no hold is performed.

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example holds all monitors and all queue transmissions.

```
Ruijie#smart manager scheduler hold all
```

The following example holds the monitor and queue transmission of the policy with the type of applet and the class B.

```
Ruijie#smart manager scheduler hold class B
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

smart manager scheduler modify

smart manager scheduler modify class *class-options* **queue-priority {high | last |low | normal}**

Parameter description

Parameter	Description
class *class-options*	Specify the class of the running policy.
queue-priority *{***high** **|last** **|low** **|normal***}*	Specify the queue priority.

Default configuration

By default, the priority of policies is **normal**.

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example sets the queue priority of the policy with the type being applet and the class being B up to high.

```
Ruijie#smart manager scheduler modify class B queue-priority high
```

Related commands

Command	Description
smart manager applet	Defined the command line based SEM policy.

smart manager scheduler release

smart manager scheduler release {all | policy *policy-id* **| class** *class-options***}**

Parameter description

Parameter	Description
all	All policies
policy *policy-id*	Specify the trigger ID of the policy.
class *class-options*	Specify the class of the running policy.

Default configuration

By default, it is release.

Command mode

Privileged EXEC mode

Usage Guideline

This command is the inverse process of the “smart manager scheduler hold”.

Examples

The following example releases all monitors and all queue transmissions.

```
Ruijie#smart manager scheduler release all
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

smart manager scheduler

In the global configuration mode, use this command to configure the thread pool of SEM policy category and set the thread pool size. The **no** form of this command is used to restore the SEM policy thread pool to the default.

smart manager scheduler thread class *class-options* **number** *thread-number*

no smart manager scheduler thread class *class-options*

Parameter description

Parameter	Description
thread class *class-options*	SEM policy category contained in the thread pool.
number *thread-number*	Number of thread in the pool.

Default configuration

By default, thread pool where the default class is has 32 threads, and no thread pool is specified for the other class.

Command mode

Global configuration mode

Usage

On condition that there is no active thread in the pool, the policy

Guideline

will be in the pending status, and it will not be switched to the active status until the active thread is available.

⚠ **Caution**

By default, the default-class thread pool has 32 available threads, while other classes have no. if the other class is used without the thread pool specified, the policy will not be executed.

Examples

The following example configures up to 5 available threads for the thread pool of Class B and Class D.

```
Ruijie(config)# smart manager scheduler thread class B D number 5
```

The following example configures up to 10 available threads for the thread pool of default-class in the policy.

```
Ruijie(config)#smart manager scheduler thread class default number 10
```

Related commands

Command	Description
Show smart manager scheduler	Show the SEM scheduler.

Platform description

N/A

smart manager scheduler suspend

In the global configuration mode, use this command to suspend the SEM scheduler. The **no** form of this command is used to restore the SEM scheduler.

smart manager scheduler suspend

no smart manager scheduler suspend

Parameter description

Parameter	Description
-	-

Default configuration

By default, the SEM scheduler is not suspended.

Command mode

Global configuration mode

Usage Guideline

Note: the running thread will not be influenced by the scheduler suspending, but continue running until the end.

Examples

The following example suspends the SEM scheduler temporarily.

```
Ruijie(config)#smart manager scheduler suspend
```

The following example restores the SEM scheduler.

```
Ruijie(config)#no smart manager scheduler suspend
```

Related commands

Command	Description
show smart manager scheduler	Show the SEM scheduler information.

trigger

Use this command to configure the trigger attributes of the policy in SEM configuration mode.

trigger [**occurs** *occurs-value*] [**occurs-period** *occurs-period-value*] [**correlate-period-start** *period-start-value*] [**correlate-period** *correlate-period-value*] [**delay** *delay-value*] [**maxrun** *maxruntime-number*]

no trigger

Parameter description

Parameter	Description
occurs *occurs-value*	(optional) matching times needed to trigger the entire policy. 1 by default.
occurs-period *occurs-period-value*	(optional) **occurs** invalid period, the duration of **occurs** operation over the period-value will be considered to time out. This parameter is invalid when the **occurs** is 1.
period-start *period-start-value*	(optional) start time of the period, it is described in the Crom method.
delay *delay-value*	(optional) the policy delays running after being triggered.
correlate-period *correlate-period-value*	(optional) the time-out period of the correlationship.
maxrun *maxruntime-number*	(optional) the maximum time to run the policy. Over this time, the policy will be forced to end. It is 20 seconds by default.

Default configuration

By default, the trigger is not configured.

Command mode

SEM mode

Usage Guideline

N/A

Examples

The following example specifies the policy named Test_1 to run with 10 seconds delay after being triggered.

```
Ruijie(config)#smart manager applet Test_1
Ruijie(config-applet)#event tag none-event none
Ruijie(config-applet)#trigger delay 10
Ruijie(config-applet)#commit
Ruijie(config-applet)#exit
```

Related commands

Command	Description
smart manager applet	Define the command line based SEM policy.

show smart manager detector

In the privileged EXEC mode, this command shows the monitor information

show smart manager detector [**all |***detector-name*] [**detailed** | **statistics**]

Parameter description

Parameter	Description
all | *detector-name*	(optional) show all monitor information or show the specific monitor information.
detailed	(optional) show the detailed information.
statistics	(optional) show the detector statistics.

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example executes the **show smart manager detector all** command:

```
Ruijie#show smart manager detector all
No.  Name             Version
1    application       01.00
2    syslog           01.00
3    cli              01.00
4    counter          01.00
5    interface         01.00
6    sysmon           01.00
7    none             01.00
8    oir              01.00
9    snmp             01.00
10   snmp-notification  01.00
11   timer            01.00
12   snmp-object       01.00
```

The following example executes the **show smart manager detecotr cli** command：

```
Ruijie#show smart manager detector cli
No.  Name             Version
1    cli              01.00
```

The following example executes the **show smart manager detector cli** detailed command.

```
Ruijie#show smart manager detector cli detailed
No.          Name          Version
1                  cli       01.00
Applet Configuration Syntax for cli detector :
       event tag <event-name> [correlate {and | or | andnot}]  cli
pattern <regular-expression> sync {yes [default <wait-time>] | no
skip {yes | no}} [mode <mode val>] [occurs <num-occurrences>] [period
<period-value>]
  no event tag <event-name>

       Applet Built-in Environment Variables:
       _event_id
```

```
_event_type
_event_type_string
_event_pub_time
_event_pub_sec
_event_pub_msec
_cli_msg
_cli_msg_count
_cli_mode
```

Related commands

Command	Description
-	-

show smart manager environment

In the privileged EXEC mode, this command shows the global variable information.

show smart manager environment [**all |** *variable-name]*

Parameter description

Parameter	Description
all | *variable-name*	(optinal) show all global variables or show the specific global variable.

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

This command shows the global variables only.

Examples

The following example executes the **show smart manager environment** command:

```
Ruijie#show smart manager environment
No.  Name                          Value
1    var_a                         value_a
2    var_b                         value_b
```

The following example executes the **show smart manager environment all** command:

```
Ruijie#show smart manager environment all
No.  Name                          Value
```

```
1   var_a                     value_a

2   var_b                     value_b
```

The following example executes the **show smart manager environment var_a**:

```
Ruijie#show smart manager environment var_a

value_a
```

The following example executes the **show smart manager environment var_none** (inexistent global variables)

```
Ruijie#show smart manager environment var_none

No such environment variable defined.
```

Related commands

Command	Description
smart manager environment	

show smart manager history events

In the privileged EXEC mode, this command shows the history information of SEM event.

show smart manager history events [detailed] [maximum *number***]**

Parameter description

Parameter	Description
detailed	(optional) show the detailed information.
maximum *number*	(optional) the maximum number to show.

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example executes the **show smart manager history events** command.

```
Ruijie#show smart manager history events
```

```
No.  Job Id Proc Status   Time of Event            Event Type
Name
1    2817   Actv success  Wed Nov11 10:15:15 2009  timer watchdog
applet: Test_1
2    2818   Actv success  Wed Nov11 10:15:17 2009  timer watchdog
applet: Test_1
3    2819   Actv success  Wed Nov11 10:15:19 2009  timer watchdog
applet: Test_1
4    2820   Actv success  Wed Nov11 10:15:21 2009  timer watchdog
applet: Test_1
5    2821   Actv success  Wed Nov11 10:15:23 2009  timer watchdog
applet: Test_1
 6    2822   Actv success  Wed Nov11 10:15:25 2009  timer watchdog
 applet: Test_1
```

The following example executes the **show smart manager history events detailed c**ommand.

```
Ruijie#show smart manager history events detailed
No.  Job Id Proc Status   Time of Event            Event Type
Name
1    2839   Actv success  Wed Nov11 10:15:59 2009  timer watchdog
applet: Test_1
 timer_time 3466923359.364 timer_remain 1.996
2    2840   Actv success  Wed Nov11 10:16:01 2009  timer watchdog
 applet: Test_1
timer_time 3466923361.364 timer_remain 1.996
3    2841   Actv success  Wed Nov11 10:16:03 2009  timer watchdog
applet: Test_1
   timer_time 3466923363.364 timer_remain 1.996
```

Related commands

Command	Description
smart manager history	

show smart manager policy all

In theprivileged EXEC mode, this command shows all policies and policy submission.

show smart manager policy all

Parameter description N/A

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

This command is used to show all configured policies.

Examples

The following example executes the **show smart manager policy all** command.

```
Ruijie#show smart manager policy all
No.  Status       Policy Name
1    commit      Test_1
2   not commit   Test_2
```

show smart manager policy registered

In the privileged EXEC mode, this command shows the policy registered.

show smart manager policy registered [statistics][policy *policy-name***][event-type** *event-name***][class** *class-options***][time-ordered |name-ordered]**

Parameter description

Parameter	Description
statistics	(optional) show the statistical information of the registered policy.
policy *policy-name*	(optional) specify the policy name.
event-type *event-name*	(optional) specify the event type of policy.
class *class-options*	(optional) select the policy class.
detailed	(optional) show the detailed information.
time-ordered | name-ordered	(optional) select the showing order.

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example executes the **show smart manager policy registered** command.

```
Ruijie#show smart manager policy registered
No.  Name     Class  Type   Event Type      Time Registered
 1  Test_1     A     applet   timer           Thu Oct 21 13:46:16
2010
event_1: timer: watchdog time 1
 action 00 syslog msg "Action_00"
 action 10 wait 360
 action 20 syslog msg "Action_20"
```

Related commands

Command	Description
smart manager applet	Define the SEM policy based on the command line.

show smart manager policy active

In the privileged EXEC mode, this command shows the actived policy instance.

show smart manager policy active [class *class-options***] [detailed]**

Parameter description

Parameter	Description
class *class-options*	(optional) select the policy class.
detailed	(optional) show the detailed information.

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

This command is used to show the policy instance being executed.

Examples

The following example executes the **show smart manager policy active** command.

```
Key: P - Priority      :L - Low, H - High, N - Normal
   S - Scheduling mode :A - Active, P -Pending

 No.  Job Id     P S Status   Time Of Event           Event Type
Policy Name
 1     3159       N  A  running   Wed  Nov11  10:28:14  2009    none
Test_1
 2     3160       N  A  running   Wed  Nov11  10:28:38  2009    none
Test_1
 3     3161       N  A  running   Wed  Nov11  10:28:38  2009    none
Test_1
 4     3162       N  A  running   Wed  Nov11  10:28:39  2009    none
Test_1
 5     3163       N  A  running   Wed  Nov11  10:28:39  2009    none
Test_1
 6     3164       N  A  running   Wed  Nov11  10:28:40  2009    none
Test_1
```

The following example executes the **show smart manager policy active detailed** command.

```
Key: P - Priority      :L - Low, H - High, N - Normal
  S - Scheduling mode :A - Active, P -Pending

 No.  Job Id     P S Status   Time Of Event           Event Type
Policy Name
 1     3159         N  A  running  Wed  Nov11  10:28:14  2009    none
Test_1
 exec time: Wed Nov11 10:28:14 2009   elapsed time 142.768
 maxrun 31536000.000
2     3160         N  A  running  Wed  Nov11  10:28:38  2009    none
Test_1
  exec time: Wed Nov11 10:28:38 2009   elapsed time 119.024
  maxrun 31536000.000
3     3161         N  A  running  Wed  Nov11  10:28:38  2009    none
Test_1
  exec time: Wed Nov11 10:28:38 2009   elapsed time 118.660
   maxrun 31536000.000
```

show smart manager policy pending

In the privileged EXEC mode, this command shows the policies of pending running.

show smart manager policy pending [class *class-options***] [detailed]**

Parameter description

Parameter	Description
class *class-options*	(optional) select the policy class.

detailed	(optional) show the detailed information.

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

Use this command to show the policies of pending running.

Examples

The following example executes the **show smart manager policy pending** command.

```
Key: P - Priority            :L - Low, H - High, N - Normal
S - Scheduling mode :A - Active, P -Pending

No.   Job  Id       P  S  Status     Time  Of  Event                  Event  Type
Policy Name
 1      3191        N  P  pend      Wed  Nov11  10:28:53  2009    none
Test_1
2      3192        N  P  pend      Wed  Nov11  10:28:53  2009    none
Test_1
 3      3193        N  P  pend      Wed  Nov11  10:28:54  2009    none
Test_1
 4      3194        N  P  pend      Wed  Nov11  10:28:54  2009    none
Test_1
 5      3195        N  P  pend      Wed  Nov11  10:28:54  2009    none
Test_1
 6      3196        N  P  pend      Wed  Nov11  10:28:55  2009    none
Test_1
```

The following example executes the **show smart manager policy pending detailed** command.

```
Key: P - Priority       :L - Low, H - High, N - Normal
 S - Scheduling mode :A - Active, P -Pending

 No.  Job Id     P  S Status   Time Of Event             Event Type
Policy Name
 1      3191        N  P  pend      Wed  Nov11  10:28:53  2009    none
Test_1
  maxrun 31536000.000
 2      3192      N  P  pend      Wed  Nov11  10:28:53  2009    none
Test_1
 maxrun 31536000.000
3     3193         N  P  pend     Wed  Nov11  10:28:54  2009    none
Test_1
 maxrun 31536000.000
 4     3194        N  P  pend     Wed  Nov11  10:28:54  2009    none
Test_1
 maxrun 31536000.000
5     3195         N  P  pend     Wed  Nov11  10:28:54  2009    none
Test_1
   maxrun 31536000.000
```

show smart manager scheduler

In the privileged EXEC mode, this command shows the operation of SEM scheduler.

show smart manager scheduler thread [**detailed**]

Parameter description

Parameter	Description
detailed	(optional) show the detailed information.

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example executes the **show smart manager scheduler thread** command.

```
Ruijie#show smart manager scheduler thread
1 Applet threads service class default :
 total: 1 running: 0 idle: 1

2 Applet threads service class A B C:
  total: 32 running: 0 idle: 32
```

The following example executes the **show smart manager scheduler thread detailed** command.

```
Ruijie#show smart manager scheduler thread detailed
```

```
 Applet threads service class default :
 total: 1 running: 0 idle: 1
2 Applet threads service class A B C:
 total: 32 running: 3 idle: 29
class A:1
calss B:2
```

show smart manager version

In the privileged EXEC mode, this command shows the version information of SEM.

show smart manager version

Parameter description

N/A

Default configuration

N/A

Command mode

Privileged EXEC mode

Usage Guideline

N/A

Examples

The following example executes the **show smart manager version** command.

```
Ruijie#show smart manager version
Smart Smart manager Version 3.10
Component Versions:
SEM: (v310_throttle)4.1.1
SEM-grtd: (v310_throttle)1.0.7
SEM-call-home: (v310_throttle)1.0.6
Event Detectors:
Name              Version
application        01.00
syslog             01.00
cli                01.00
counter            01.00
interface         01.00
sysmon             01.00
none              01.00
```

```
oir               01.00
snmp              01.00
snmp-notification 01.00
timer             01.00
snmp-object       01.00
```

VSU Configuration Commands

dual-active detection

Configure dual-active detection function. The **no** form of this command is used to restore the default configuration.

dual-active detection { **aggregateport** | **bfd** }

no dual-active detection { **aggregateport** | **bfd** }

Parameter Description

Parameter	Description
aggregateport	Specify the aggregate port detection mode.
bfd	Specify the Bidirectional Forwarding Direction (BFD) mode.

Default Configuration

The dual-active detection is disabled by default.

Command Mode

config-vs-domain configuration mode

Usage Guidelines

This command can only be executed in VSU mode.

Configuration Examples

Example 1 enables BFD dual-active detection.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active detection bfd
```

Example 2 disables BFD dual-active detection.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# no dual-active detection bfd
```

Example 3 enables aggregate port dual-active detection.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active detection aggregateport
```

Example 4 disables aggregate port dual-active detection.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# no dual-active detection aggregateport
```

Related Commands

Command	Description
dual-active interface	Configure AP-based dual-active detection interfaces.

dual-active bfd interface	Configure BFD dual-active detection interfaces.
dual-active exclude interface	Configure the exclude interface of dual-active detection.
show switch virtual dual-active	Check the configuration and status of the dual-active detection function.

Platform Description

N/A

dual-active exclude interface

Configure the exclude interface of VSU in the recovery mode. The **no** form of this command is used to cancel the exclude interface.

dual-active exclude interface *interface-name*

no dual-active exclude interface *interface-name*

Parameter Description

Parameter	**Description**
interface-name	Indicates the interface type and number

Default Configuration

N/A

Command Mode

config-vs-domain configuration mode

Usage Guidelines

This command can only be executed in the VSU mode.

The exclude interface must be a routing interface but not a VSL interface.

Users can configure multiple exclude interfaces.

Configuration Examples

The following example configures Gi 1/0/3 as the exclude interface of dual-active detection.

```
Ruijie(config)# interface GigabitEthernet 1/0/3
Ruijie(config-if)# no switchport
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active exclude interface GigabitEthernet 1/0/3
```

Related Commands

Command	**Description**
dual-active detection	Configure the functional switch of dual-active detection.
dual-active bdf interface	Configure the interface of BFD dual-active detection to detect the dual-active device status.
dual-active interface	Configure the interface of aggregate port dual-active detection to detect the dual-active device status.
show switch virtual dual-active	Check the configuration and status of the dual-active

	detection function.

Platform Description

N/A

dual-active bfd interface

Configure the bfd detection interface. The **no** form of this command is used to cancel the detection interface.

dual-active interface *interface-name*

no dual-active bfd interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Indicates the interface type and number

Default Configuration

-

Command Mode

config-vs-domain configuration mode

Usage Guidelines

The BFD detection interfaces must be routed ports on different devices.

Configuration Examples

The following example configures Gi1/1/1 port as the BFD dual-active detection interface.

```
Ruijie(config)# interface GigabitEthernet 1/1/1
Ruijie(config-if)# no switchport
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/1/1
```

Related Commands

Command	Description
dual-active detection	Configure the functional switch of dual-active detection.
show switch virtual dual-active	Check the configuration and status of the dual-active detection function.

Platform Description

N/A

dual-active interface

Use this command to configure AP-based dual-active detection interfaces. Use the **no** form of this command is used to delete the detection interfaces.

dual-active interface *interface-name*

no dual-active interface

Parameter Description

Parameter	Description
interface-name	Indicates the type and number of detection interface. The interface must be an AP type.

Default Configuration

N/A

Command Mode

config-vs-domain configuration mode

Usage Guidelines

You can configure only one AP-based dual-active detection interface. Before setting the AP port as the detection interface, create the interface. The latter configured detection interface will cover the formerly configured one.

Configuration Examples

The following example configures aggregate port 1 as a detection interface.

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#exit
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# dual-active interface aggregateport 1
```

Related Commands

Command	Description
dual-active detection	Configure the functional switch of dual-active detection.
show switch virtual dual-active	Check the configuration and status of the dual-active detection function.

Platform Description

N/A

dad relay enable

Use this command to configure AP-based detection dual-active forwarding function. Use the **no** form of this command to disable the forwarding function.

dad relay enable

no dad relay enable

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration

The AP-based detection dual-active forwarding function is disabled by default.

Command Mode

Interface configuration mode

Usage Guidelines

This command can only be executed on the AP interface.

Configuration Examples

#Enable relay function.

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#dad relay enable
```

#Disable relay function.

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#no dad relay enable
Ruijie(config-if-AggregatePort 1)#exit
```

Related Commands

Command	Description
dual-active detection	Configure dual-active detection.
dual-active bfd interface	Configure BFD dual-active detection interfaces.
dual-active interface	Configure AP-based dual-active detection interfaces
dual-active exclude interface	Configure the exclude interface of dual-active detection.
show switch virtual dual-active	Check the configuration and status of the dual-active detection function.

Platform Description

N/A

port-member interface

Configure a VSL-AP member interface. The **no** form of this command is used to remove the member interface.

port-member interface *interface-name* [**copper** | **fiber**]

no port-member interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Indicates the name of a two-dimensional interface, such as GigabitEthernet 0/1 and GigabitEthernet 0/3.
copper	Indicates electrical port attribute.

fiber	Indicates optical port attribute.

Default Configuration

N/A

Command Mode

config-vsl-ap configuration mode

Usage Guidelines

This command can be executed in both the VSU and standalone modes.

This command takes effect only after you save the command configuration and reload the device where the VSL member ports are.

Configuration Examples

#Add/remove a VSL-AP member port in the standalone mode.

```
Ruijie(config)# vsl-aggregateport 1
Ruijie(config-vsl-ap-1)# port-member interface GigabitEthernet 0/1
Ruijie(config-vsl-ap-1)# no port-member interface GigabitEthernet 0/2
```

#Add/remove a VSL-AP member port in the VSU mode.

```
Ruijie(config)# vsl-aggregateport 1/1
Ruijie(config-vsl-ap-1/1)# port-member interface GigabitEthernet 0/1
Ruijie(config-vsl-ap-1/1)# no port-member interface GigabitEthernet 0/1
```

Related Commands

Command	Description
vsl-aggregateport	Enter the vsl-ap configuration mode.

Platform Description

N/A

remove configuration switch

Remove the configuration of a specific device and automatically restart the device.

remove configuration switch *sw_id*

Parameter Description

Parameter	Description
sw_id	Indicates the ID of a switch in VSU. The value range is 1 to 8.

Default Configuration

N/A

Command Mode

Global configuration mode

Usage

This command can only be executed in the VSU mode and cannot be used to remove the

Guidelines

configuration of the master device.

Configuration Examples

#Remove the configuration of Switch 3.

```
Ruijie(config)# remove configuration switch 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

session

Use this command to configure redirection to the console of the master or any device.

session { **device** *sw_id* | **master** }

Parameter Description

Parameter	Description
device	Configure redirection to the console of the member device.
sw_id	Member device ID, in the range of 1 to 8.
master	Configure redirection to the master console.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Usage Guidelines

This command can be used in VSU mode.

Configuration Examples

#Configure redirection from the serial port console of the slave device 2 to the master console, and then exit .

```
Ruijie-STANDBY-2#session master
Ruijie#exit
Ruijie-STANDBY-2
```

#Configure redirection from the master console to the device 2 console, and then exit.

```
Ruijie#session device 2
Ruijie-STANDBY-2>#exit
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show switch id

Show the switch ID.

show switch id

Parameter Description

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

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Usage Guidelines

This command can be executed in both the VSU and standalone modes. The current switch ID can be viewed in the VSU mode and the currently configured switch ID can be viewed in the standalone mode.

Configuration Examples

#Show the currently configured switch ID in the standalone mode.

```
Ruijie #show switch id
Switch ID is 2
```

#Show the current switch ID in the VSU mode.

```
Ruijie#show switch id
Switch ID is 1
```

Related Commands

Command	Description
show switch virtual	Show the domain ID, the ID and the role of each device.

Platform Description

N/A

show switch virtual

Show the domain ID, the ID, status and role of each device.

show switch virtual

Parameter

Parameter	**Description**

Description

N/A	N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Usage Guidelines

N/A

Configuration Examples

#Example 1: standalone mode

```
Ruijie# show switch virtual
Current system is running in "STANDALONE" mode.
```

#Example 2: VSU mode, three member switches

```
Ruijie#show switch virtual
Switch_id     Domain_id     Priority     Status     Role
---------------------------------------------------------
1(1)          1(1)          100(100)     OK         ACTIVE       switch-1
2(2)          1(1)          100(100)     OK         CANDIDATE    switch-2
3(3)          1(1)          100(100)     OK         STANDBY      switch-3
```

Related Commands

Command	Description
switch	Configure the switch ID.
switch *sw_id* **priority**	Configure the switch priority.
switch *sw_id* **renumber**	Modify the switch ID.
switch *sw_id* **domain**	Modify the domain ID.
switch virtual domain	Configure the VSU virtual switch ID.

Platform Description

N/A

show switch virtual balance

Show the traffic balancing configuration in the VSU mode.

show switch virtual balance

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Usage Guidelines

N/A

Configuration Examples

#Show the traffic balancing configuration of the current switch in the VSU mode.

```
Ruijie#show switch virtual balance
Aggregate port LFF: enable
```

Related Commands

Command	Description
show switch virtual	Show the domain ID, ID and role of every device.

Platform Description

N/A

show switch virtual config

Show the VSU configuration information in the standalone or VSU mode.

show switch virtual config [*sw_id*]

Parameter Description

Parameter	Description
sw_id	Switch ID Show the VSU configuration information of a specified device.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Usage Guidelines

N/A

Configuration Examples

#Show the VSU configuration information of the current switch in the standalone mode.

```
Ruijie#show switch virtual config
switch_id: 1 (mac: 00d0.f810.3323)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
switch convert mode standalone
!
```

#Show the VSU configuration information in the VSU mode.

```
Ruijie#show switch virtual config
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
switch 1 description switch1
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

switch_id: 2 (mac: 00d0.f810.2222)
!
switch virtual domain 1
!
switch 2
switch 2 priority 100
switch 2 description switch2
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
```

Example 3 shows the VSU configuration information in the VSU mode.

```
Ruijie#show switch virtual config 1
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
```

```
switch 1
switch 1 priority 200
switch 1 description switch1
!
vsl-aggregateport 1
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
```

Related Commands

Command	Description
show switch virtual	Show the domain ID, the ID and role of each device.

Platform Description

N/A

show switch virtual dual-active

Show the information of dual-active detection.

show switch virtual dual-active { **aggregateport** | **bfd** | **summary** }

Parameter Description

Parameter	Description
aggregateport	Show the AP-based detection information.
bfd	Show the BFD-based detection information.
summary	Show brief DAD information.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Usage Guidelines

N/A

Configuration Examples

Example 1 checks the configuration and status of the dual-active detection.

```
Ruijie# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: No
Interfaces excluded from shutdown in recovery mode:
GigabitEthernet 1/0/3
GigabitEthernet 1/0/4
```

```
In dual-active recovery mode: No
```

Example 2 checks the configuration information of BFD dual-active detection.

```
Ruijie# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
    GigabitEthernet 1/0/1: UP
    GigabitEthernet 2/0/2: UP
```

Example 3 checks the status of AP-based dual-active detection.

```
Ruijie# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
    AggregatePort 1:  UP
        GigabitEthernet 1/0/1: UP
        GigabitEthernet 2/0/1: UP
        GigabitEthernet 1/0/2: UP
        GigabitEthernet 2/0/2: UP
DAD relay enable AP list:
    AggregatePort 1
```

Related Commands

Command	Description
dual-active detection	Turn on the dual-active detection switch.
dual-active interface	Configure AP-based dual-activedetection interfaces.
dual-active bfd interface	Configure BFD dual-active detection interfaces.
dual-active exclude interface	Configure the exclude interface.

Platform Description

N/A

show switch virtual link

Show VSL status information.

show switch virtual link [**port**]

Parameter Description

Parameter	Description
port	Show the status information of VSL sub-interface.

Default Configuration

N/A

Command

Privileged EXEC mode

Mode

Usage Guidelines

N/A

Configuration Examples

Example 1 shows the information of VSL convergence link.

```
Ruijie# show switch virtual link
VSL-AP   State    Peer-VSL      Rx       Tx       Uptime
----------------------------------------------------------------------------------
1/1      UP       2/1           100000   100000    1d,4h,29m
2/1      UP       1/1           100000   100000    1d,4h,29m

VSL Status has two values: DOWN and UP.
```

Example 2 shows the VSL port information.

```
Ruijie# show switch virtual link port
VSL-AP-1/1:
Port                   State    Peer-port              Rx   Tx   Uptime
-----------------------------------------------------------------------------------
GigabitEthernet 1/0/1  OK       GigabitEthernet 2/0/1  9000 9000 0d,0h,20m
GigabitEthernet 1/0/2  OK       GigabitEthernet 2/0/2  9000 9000 0d,0h,20m

VSL-AP-2/1:
Port                   State    Peer-port              Rx   Tx   Uptime
-----------------------------------------------------------------------------------
GigabitEthernet 2/0/1  OK       GigabitEthernet 1/0/1  9000 9000 0d,0h,20m
GigabitEthernet 20/2   OK       GigabitEthernet 1/0/2  9000 9000 0d,0h,20m
```

Related Commands

Command	**Description**
show switch virtual	Show VSU system information.

Platform Description

N/A

show switch virtual topology

Show the topology connection status of VSU system.

show switch virtual topology

Parameter Description

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

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Usage Guidelines

N/A

Configuration Examples

Example 1 shows the topology status.

```
Ruijie# show switch virtual topology
Ring Topology:
[1]---[2]---[3]---[4]---[5]---[6]---[1]

switch[1] (mac: 001a.a97e.0ecf, description: switch1):
    vsl-ap[1] <--> vsl-ap[2] of switch[6]
    vsl-ap[2] <--> vsl-ap[1] of switch[2]

switch[2] (mac: 001a.a97e.0ed1, description: switch2):
    vsl-ap[1] <--> vsl-ap[2] of switch[1]
    vsl-ap[2] <--> vsl-ap[1] of switch[3]

switch[3] (mac: 001a.a97e.0ed2, description: switch3):
    vsl-ap[1] <--> vsl-ap[2] of switch[2]
    vsl-ap[2] <--> vsl-ap[1] of switch[4]

switch[4] (mac: 001a.a97e.0ed3, description: switch4):
    vsl-ap[1] <--> vsl-ap[2] of switch[3]
    vsl-ap[2] <--> vsl-ap[1] of switch[5]

switch[5] (mac: 001a.a97e.0ed4, description: switch5):
    vsl-ap[1] <--> vsl-ap[2] of switch[4]
    vsl-ap[2] <--> vsl-ap[1] of switch[6]

switch[6] (mac: 001a.a97e.0ed5, description: switch6):
    vsl-ap[1] <--> vsl-ap[2] of switch[5]
    vsl-ap[2] <--> vsl-ap[1] of switch[1]
```

Related Commands

Command	Description
switch *sw_id* **priority**	Configure the priority of a switch in VSU.
switch virtual domain	Configure the VSU virtual switch ID.
show switch virtual link	Check the VSL information.

Platform Description

N/A

switch

Specify the ID of a device in the VSU system. The **no** form of this command is used to restore the default value.

switch *sw_id*

no switch

Parameter Description

Parameter	Description
sw_id	Indicates the ID of a device in VSU. The value range is 1 to 8.

Default Configuration

The default ID is 1.

Command Mode

config-vs-domain configuration mode

Usage Guidelines

Every member device in a VSU system has an ID. In the VSU mode, the interface name changes from **slot/port** into **switch/slot/port** format, where the **switch** is the switch ID that the interface locates.

To select the master device, if two devices are master devices or the two devices have no role and have the same priority, select the device with a smaller ID as the master device.

This command can only be executed in the standalone mode to modify a switch ID. In the VSU mode, use **switch** *sw_id* **renumber** *new_sw_id* to modify a switch ID. No matter in the standalone mode or VSU mode, the modified switch ID becomes valid after the device restarts.

Configuration Examples

Example 1 specifies the switch ID to 2 in the VSU where the domain ID is 1.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 2
```

Related Commands

Command	Description
switch virtual domain	Specify the VSU virtual switch ID.
switch *sw_id* **priority** *priority_num*	Configure the priority of a switch in VSU.
show switch virtual	Show the domain ID, the ID and role of each device.

Platform Description

N/A

switch *sw_id* description

Configure the description of a switch in VSU. The **no** form of this command is used to empty the descriptor.

switch *sw_id* **description** *dev-name*

no switch *sw_id* **description**

Parameter Description

Parameter	Description
sw_id	Indicates the ID of the switch that needs to be configured with a priority.
dev_name	Indicates the device name description

Default Configuration

N/A

Command Mode

config-vs-domain configuration mode

Usage Guidelines

The command can be executed in the standalone and VSU modes. The configuration becomes valid immediately in the VSU mode.

Configuration Examples

#Example:

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 description buildingA
Ruijie(config-vs-domain)# exit
```

Related Commands

Command	Description
switch	Configure a switch ID.
show switch virtual	Show the domain ID, the ID and role of each device.

Platform Description

N/A

switch *sw_id* domain

Modify the domain ID of any switch in the VSU mode. The **no** form of this command is used to restore the default value.

switch *sw_id* **domain** *new_domain_id*

no switch *sw_id* **domain**

Parameter Description

Parameter	Description
sw_id	Indicates the ID of the currently running switch in the VSU mode. The value rang is 1 to 8.
new_domain_id	Indicates the modified domain ID. The value range is 1 to 255.

Default Configuration

100

Command Mode

config-vs-domain configuration mode

Usage Guidelines

This command can only be executed in the VSU mode instead of the standalone mode. The configuration becomes valid only after the device restarts.

The **no** form of this command is used to restore the default value **100** of the domain ID.

Configuration Examples

#Modify the domain ID of Switch 1 to **10** in the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 domian 10
```

#Modify the domain ID of Switch 2 to **10** in the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 2 domian 10
```

#Modify the domain ID of Switch 2 to the default value in the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# no switch 2 domain
```

Related Commands

Command	Description
switch virtual domain	Specify the VSU virtual switch ID.
show switch virtual	Check the domain ID, the ID and role of each device.

Platform Description

N/A

switch *sw_id* priority

Configure the priority of a switch in VSU. The **no** form of this command is used to restore the default value.

switch *sw_id* **priority** *priority_num*

no switch *sw_id* **priority**

Parameter Description

Parameter	Description
sw_id	Indicates the ID of the switch that needs to be configured with a priority.
priority_num	Indicates the priority of the corresponding switch. The value range is 1-255.

Default Configuration

priority_num：The default priority number is 100.

Command Mode

config-vs-domain configuration mode

Usage Guidelines

This bigger the number is, the higher the priority is. Select the device that has the highest priority as the master device.

This command can be executed in both the VSU and standalone modes. The configuration becomes valid only after the device restarts.

This command cannot modify *sw_id.* In the standalone mode, if *sw_id* is set to **1**, running the **switch 2 priority 200** command does not work. You can first use switch 2 to modify *sw_id* to **2** and then run the **switch 2 priority 200** command. In the VSU mode, *sw_id* indicates the ID of the currently running switch. If the ID does not exist, the configuration does not become valid.

Configuration Examples

#Configure the priority of Switch 1 to **200** in the standalone mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# exit
```

# Modify the priority of Switch 1 to **200** and restore the default value of the priority of Switch 2 in the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# no switch 2 priority
Ruijie(config-vs-domain)# exit
```

Related Commands

Command	Description
switch	Configure a switch ID.
show switch virtual	Show the domain ID, the ID and role of each device.

Platform Description

N/A

switch *sw_id* renumber

Modify the ID of any switch in the VSU mode. The **no** form of this command is used to restore the default value.

switch *sw_id* **renumber** *new_sw_id*

no switch *sw_id*

Parameter Description

Parameter	Description
sw_id	Indicates the ID of the currently running device in the VSU mode. The value rang is 1 to 8.
new_sw_id	Indicates the modified switch ID.

Default Configuration

1

Command Mode

config-vs-domain configuration mode

Usage Guidelines

This command can only be executed in the VSU mode instead of the standalone mode. The configuration becomes valid only after the device restarts.

The **no** form of this command is used to restore the default value **1** of *sw_id*.

Configuration Examples

#Modify the ID of Switch 1 to **2** in the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1 renumber 2
```

#Modify the ID of Switch 2 to the default value in the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# no switch 2
```

Related Commands

Command	Description
switch	Configure a switch ID in the standalone mode.
show switch virtual	Check the domain ID, the ID and role of each device.

Platform Description

N/A

switch convert mode

Perform a handover between the standalone and VSU modes.

switch convert mode { **virtual** | **standalone** [*sw_id*] }

Parameter Description

Parameter	Description
virtual	Shift into the VSU mode.
standalone	Shift into the standalone mode.
sw_id	Indicates the switch ID

Default Configuration

The switch operates in the standalone mode by default.

Command Mode

Privileged EXEC mode

Usage

- After the **switch convert mode virtual** command is run, the software automatically backs up

Guidelines

the configuration file in the standalone mode as **standalone.text**, removes the configuration file **config.text**, prompts the user to decide whether to overwrite **config.text** with **virtual_switch.text**, write related configurations of VSU in **config_vsu_dat**, and finally restarts the switch.

- After the **switch convert mode standalone** command is run, the master device backs up the configuration file in the VSU mode as **virtual_switch.text**, removes the configuration file **config.text**, prompts the user to decide whether to overwrite **config.text** with **standalone.text**, writes related configurations of VSU in **config_vsu_dat**, and finally restarts the switch.
- This command can be executed in both the standalone and VSU modes. If the command is run in the standalone mode, the current device performs the standalone/VSU mode handover. If the command contains a switch ID and is run in the VSU mode, the switch with the ID performs the standalone/VSU mode handover. If the command does not contain a switch ID, the master device performs a handover. It is advised to perform standalone/VSU mode handover on the slave device and then on the master device.

Configuration Examples

#In the standalone mode, configure the domain ID to **1**, the switch ID to **1** and the switch priority to **200** and then convert the switch from standalone mode to VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch 1
Ruijie(config-vs-domain)# switch 1 priority 200
Ruijie(config-vs-domain)# end
Ruijie# switch convert mode virtual
```

#In the VSU mode, convert the slave device (The sw_id is 2) to the standalone mode and then convert the master device (The sw_id is 1) to the standalone mode.

```
Ruijie# switch convert mode standlone 2
Ruijie# switch convert mode standlone 1
```

Related Commands

Command	**Description**
switch *num*	Specify a device ID in VSU
switch virtual domain	Specify the VSU virtual device ID.
switch *number* **priority** *priority_num*	Configure the priority of a switch in VSU.
show switch virtual	Check the domain ID, the ID and role of each device.

Platform Description

N/A

switch virtual aggregateport-lff enable

Enable the local priority forwarding feature of AP in the VSU mode. The **no** form of this command is used to disable the local priority forwarding feature, namely, to change into the cross-switch traffic balancing mode.

switch virtual aggregateport lff enable

no switch virtual aggregateport lff enable

Parameter Description

Parameter	Description
N/A	N/A

Default Configuration

The local priority forwarding feature is enabled by default.

Command Mode

config-vs-domain configuration mode

Usage Guidelines

N/A

Configuration Examples

#Enable the local priority forwarding feature of AP in the VSU mode.

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)# switch virtual aggregateport-lff enable
```

Related Commands

Command	**Description**
show switch virtual balance	Check the current traffic balancing mode.

Platform Description

N/A

switch virtual domain

Configure the VSU domain ID. The **no** form of this command is used to restore the default value.

switch virtual domain *number*

no switch virtual domain

Parameter Description

Parameter	**Description**
number	Indicates the VSU domain ID.

Default Configuration

The domain ID is **100** by default.

Command Mode

config-vs-domain configuration mode

Usage Guidelines

Only two devices that have the same domain ID can form a VSU system. The domain ID must be unique in a WLAN.

Configuration

Configure the domain ID to **1**.

Examples

```
Ruijie(config)# switch virtual domain 1
Ruijie(config-vs-domain)#
```

Related Commands

Command	Description
show switch virtual	Check the VSU information.

Platform Description

N/A

vsl-aggregateport

Enter the VSL-AP configuration mode.

vsl-aggregateport *ap_num*

vsl-aggregateport *sw_id/ap_num*

Parameter Description

Parameter	Description
ap_num	Indicates the VSL-AP number. The value range is 1 to 2.
sw_id	Indicates the switch ID. The value range is 1 to 8.

Default Configuration

N/A

Command Mode

config configuration mode

Usage Guidelines

This command can be executed in both the standalone and VSU modes. The *sw_id/ap_num* parameter can only be used in the VSU mode and the *ap_num* parameter can be used in the standalone mode.

The *ap-num* of VSL does not occupy the global AP of a switch.

Configuration Examples

#Enter the VSL-AP configuration mode in the standalone mode.

```
Ruijie(config)# vsl-aggregateprot 1
Ruijie(config-vsl-ap-1)#
```

#Enter the VSL-AP configuration mode in the VSU mode.

```
Ruijie(config)# vsl-aggregateprot 1/1
Ruijie(config-vsl-ap-1/1)#
```

Related Commands

Command	Description
port-member interface	Add/remove a VSU-AP member interface.

Platform Description

N/A

Network Management and Monitoring

1. SNMP Configuration Commands
2. RMON Configuration Commands
3. NTP Configuration Commands
4. SNTP Configuration Commands
5. SPAN Configuration Commands
6. RSPAN Configuration Commands

SNMP Configuration Commands

no snmp-server

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

no snmp-server

Parameter Description

Parameter	**Description**
-	-

Defaults

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 example below disables the SNMP agent service.

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

Related Commands

Command	**Description**
-	-

Platform Description

-

show snmp

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

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

Parameter Description

Parameter	**Description**
-	-

Defaults

-

Command Mode

Privileged EXEC mode.

Usage Guide

show snmp: Show the SNMP information.

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 configuration set by users.

Configuration Examples

The example below shows the SNMP information:

```
Ruijie# show snmp
Chassis: 60FF60
0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 SNMP packets output
0 Too big errors (Maximum packet size 1472)
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
```

Related Commands

Command	Description
snmp-server *chassis-id*	Specify the SNMP system sequence number.

Platform Description

-

snmp trap link-status

Use this command to configure in a device whether to send LinkTrap of the interface based on the interface configuration. When this function is enabled, SNMP will send LinkTrap if the link status of the interface changes; otherwise, it will not send LinkTrap. When the **no** form of this command is used, SNMP will not send LinkTrap.

snmp trap link-status

no snmp trap link-status

Parameter Description

Parameter	Description
-	-

Defaults

By default, this function is enabled. If the link status of the interface changes, SNMP will send LinkTrap.

Command Mode

Interface configuration mode

Usage Guide

This command is used to configure whether to send LinkTrap of an interface, such as the Ethernet interface, AP interface and SVI interface. When the function is enabled, if the link status of the interface changes, SNMP will send LinkTrap; otherwise, it will not.

Configuration Examples

Example 1: Configure not to send LinkTrap of the interface:

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# no snmp trap link-status
```

Example 2: Configure to send LinkTrap of the interface:

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if)# snmp trap link-status
```

Related Commands

Command	Description
-	-

Platform Description

-

snmp-server chassis-id

Use this command to specify the SNMP system sequential number in global configuration mode. The **no** form of this command is used 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 sequential number, numerals or characters.

Defaults

The default sequence number is 60FF60.

Command Mode

Global configuration mode.

Usage Guide

The SNMP system sequence number is generally the sequence number of the machine to facilitate the device identification. The sequence number can be viewed through the **show snmp** command.

Configuration Examples

The example below specifies the SNMP system sequence number as 123456:

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

Related Commands

Command	Description
show snmp	Show the SNMP information.

Platform Description

-

snmp-server community

Use this command to specify the SNMP community access string in global configuration mode. The **no** format of the command cancels the SNMP community access string.

snmp-server community [**0** | **7**] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [**ipv6** *ipv6-aclname*] [*aclnum*] [*aclname*]

no snmp-server community [**0** | **7**] *string*

Parameter Description

Parameter	Description
0	It indicates that the entered community string is in plaintext.
7	It indicates that the entered community string is in ciphertext.
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 management
ro	Indicate that the NMS can only read the variables of the MIB.
rw	Indicate that the NMS can read and write the variables of the MIB.
aclnum	Sequence number of the ACL, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.

ipv6-aclname	Name of the IPv6 ACL, which specifies the IPv6 address range of the NMS that are permitted to access the MIB
ipaddr	IP address of the NMS accessing the MIB

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,use the **no snmp-server** command.

If the **service password-encryption** command is configured globally and the entered community string is in plaintext, this command will display and store the community string as a ciphertext. In this case, after the configuration of the **service password-encryption** command is removed, the community string is still displayed and stored as a ciphertext rather than a plaintext.

Configuration Examples

The example below restricts the access to the MIB through 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	Define the access list.
service password-encryption	Display the password in ciphertext.

Platform Description

-

snmp-server contact

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

snmp-server contact *text*

no snmp-server contact

Parameter Description

Parameter	Description
text	String describing the system contact.

Defaults

N/A.

Command

Global configuration mode.

Mode

Configuration Examples

The example below specifies the SNMP system contract i-net800@i-net.com.cn:

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

Related Commands

Command	Description
show snmp-server	Check the SNMP information.
no snmp-server	Disable the SNMP agent function.

Platform Description

-

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. The **no** form of this command is used 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	Enable the trap notification of SNMP events.

Defaults

Disabled.

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 example below 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	Specify the SNMP host to send the SNMP Trap message.

Platform Description

-

snmp-server group

Use this command to set the SNMP user group in 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	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 to only SNMPv3.
priv	Authenticate and encrypt the messages transmitted by the user group. This applies to only SNMPv3.
readview	Associate with a read-only view.
aclnum	Sequence number of the ACL in the range of 1 to 99, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 ACL, which specifies the IPv6 address range of the NMS that are permitted to access the MIB.
writeview	Associate with a read-write view.

Defaults N/A.

Command Mode Global configuration mode.

Usage Guide -

Configuration Examples The example below sets a user group.

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

Related Commands

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

Platform Description -

snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message in global configuration mode. The **no** form of this command is used 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	Set 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

By default, no SNMP host is specified.

If no type of the SNMP trap message is specified, all types of the SNMP trap message will be 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**.

It is possible to configure multiple SNMP hosts to receive the SNMP Trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages have to be configured.

Configuration Examples

The example below 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	Enable to send the SNMP trap message.

Platform Description

-

snmp-server location

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

snmp-server location *text*

no snmp-server location

Parameter Description

Parameter	Description
text	String describing the system

Defaults Null

Command Mode Global configuration mode.

Configuration Examples The example below specifies the system information:

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

Related Commands

Command	Description
snmp-server contact	Specify the system contact information.

Platform Description -

snmp-server net-id

Use this command to set the device network element code information in global configuration mode. Use the **no** form of this command to delete the network element code information.

snmp-server net-id *text*

no snmp-server net-id

Parameter Description

Parameter	Description
net-id *text*	Set the device network element code *text*, which is a character string with the length of 1 to 255. It is case sensitive and can contain spaces.

Defaults The device network element code information is null.

Command Mode Global configuration mode

Usage Guide -

Configuration Examples The following example sets a device network element code:

```
Ruijie(config)# snmp-server net-id FZ_CDMA_MSC1
```

Related Commands

Command	Description
-	-

Platform Description -

snmp-server packetsize

Use this command to specify the maximum size of the SNMP packet in global configuration mode. The **no** form of this command is used 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 of 484 to 17876 bytes

Defaults 1472 bytes.

Command Mode

Global configuration mode.

Usage Guide

-

Configuration Examples

The example below specifies the maximum SNMP packet size as 1,492 bytes:

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

Related Commands

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

Platform Description

-

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 of 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 example below specifies the speed to send the trap message to 4 messages per second:

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

Related Commands

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

Platform Description

-

snmp-server system-shutdown

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

snmp-server system-shutdown

no snmp-server system-shutdown

Parameter Description

Parameter	Description
-	-

Defaults Disabled.

Command Mode Global configuration mode.

Usage Guide 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 pending before the device is reloaded or rebooted.

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

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

Related Commands

Command	Description
-	-

Platform Description -

snmp-server trap-format private

Use this command to set the SNMP Trap message to carry private fields in global configuration mode. Use the **no** form of this command to restore the default setting.

snmp-server trap-format private

no snmp-server trap- format private

Parameter Description

Parameter	Description
-	-

Defaults The information carries no private field.

Command Global configuration mode

Mode

Usage Guide

This command is used to configure the Trap message to carry fields in private formats. The fields include serial numbers of alarms, identification names of NE, original levels and types of alarms, reason numbers and reasons of alarms, and time, status, titles and contents of alarms. For specific data types and ranges of each field, please read RUIJIE-TRAP-FORMAT-MIB.mib.

Note The configuration does not take effect when SNMP v1 is used to send a Trap message.

Configuration Examples

The following example specifies a Trap message to carry private fields:

```
Ruijie(config)# snmp-server trap-format private
```

Related Commands

Command	Description
snmp-server enable traps	Enable the function of sending Trap message initiatively.
snmp-server host	Specify a host for NMS.

Platform Description

-

snmp-server trap-source

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

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter Description

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

Defaults

The IP address of the interface where the NMP message is sent from is just the source address.

Command Mode

Global configuration mode.

Usage Guide

By default, the IP address of the interface where the NMP message is sent from is just the source address. For easy management and identification, this command can be used to fix a local IP address as the SNMP source address.

Configuration Examples

The example below 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	Enable the sending of the SNMP trap message.
snmp-server host	Specify the NMS host to send the SNMP trap message.

Platform Description

-

snmp-server trap-timeout

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

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter Description

Parameter	Description
seconds	Timeout (in seconds) of retransmit the SNMP trap message. Range: 1 to 1000.

Defaults

30 seconds.

Command Mode

Global configuration mode.

Configuration Examples

The example below specifies the timeout period as 60 seconds.

```
Ruijie(config)# snmp-server trap-timeout 60
```

Related Commands

Command	Description
snmp-server queue-length	Specify the length of the SNMP trap message queue.
snmp-server host	Specify the NMS host to send the SNMP trap message.
snmp-server trap-source	Specify the source address for the SNMP Trap message.

snmp-server udp-port

Use this command to specify the number of the protocol port to receive SNMP packets in global configuration mode. Use the **no** form of this command to remove the configuration and use the default protocol port 161 to receive SNMP packets.

snmp-server udp-port *port-num*

no snmp-server udp-port

Parameter Description

Parameter	Description
port-num	Specify the number of the protocol port to receive SNMP packets.

Defaults

By default, the protocol port 161 is used to receive SNMP packets.

Command Mode

Global configuration mode

Usage Guide

-

Configuration Examples

The following example specifies the protocol port 15000 to receive SNMP packets:

```
Ruijie(config)# snmp-server udp-port 15000
```

Related Commands

Command	Description
-	-

Platform Description

-

snmp-server user

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

snmp-server user *username groupname* { **v1 | v2c | v3** [**encrypted**] [**auth** { **md5 | sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { [**ipv6** *ipv6_aclname*] [*aclnum* | *aclname* }]]

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

Parameter Description

Parameter	Description
username	User name
groupname	Group name of the user.
v1 | v2c | v3	SNMP version. But only SNMPv3 supports the following security parameters.

encrypted	Input the password in cipher text mode. In cipher text mode, input continuous HEX alphanumeric characters. Note that the authentication password of MD5 has a length of 16 characters, 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	Specify whether to use the authentication.
auth-password	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
priv	Encryption mode. des56 refers to 56-bit DES encryption protocol. priv-password: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
md5	Enable the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
aclnumber	Sequence number of the ACL in the range of 1 to 99, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
aclname	Name of the ACL, which specifies the IPV4 address range of the NMS that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 ACL, which specifies the IPv6 address range of the NMS that are permitted to access the MIB

Defaults

N/A.

Command Mode

Global configuration mode.

Usage Guide

-

Configuration Examples

The example below 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	Show the SNMP user configuration.

Platform Description

-

snmp-server view

Use this command to set a SNMP view in global configuration mode**.** The **no** form of this command is used 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	Specify the MIB object to associate with the view.
include	Include the sub trees of the MIB object in the view.
exclude	Exclude the sub trees of the MIB object from the view.

Defaults

By default, a default view is set to access all MIB objects.

Command Mode

Global configuration mode.

Usage Guide

-

Configuration Examples

The example below 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	Show the view configuration.

Platform Description

-

RMON Configuration 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*

Parameter Description

Parameter	**Description**
Number	The index number of the warning entry, in range of 1 to 65535.
Variable	Warning variable, a character string composed of 1 to 255 characters, in the OID dotted format (the format is entry.integer.instance or leave node.instance, for example,1.3.6.1.2.1.2.1.10.1).
Interval	Sampling interval, in range of 1 to 2147483647, in second.
Absolute	The sampling type is absolute value sampling. When the sampling time is up, the system will draw the variable
delta	The sampling type is changed value sampling .When the sampling time is up, the system will draw the changing values during the sampling interval.
rising-threshold *valueevent-number*	Set as the *value* of the upper limit and the corresponding *event number*: Range of *value*: -2147483648 to +2147483647 Range of *event-number* : 1 to 65535
falling-threshold *value event-number*	Set the value of the lower limit and the corresponding event number. Range of *value*: -2147483648 to +2147483647 Range of *event number*:: 1 to 65535
owner*ownername*	Set the entry *ownername*, in a character string composed of 1 to 64 characters, the character string is case sensitive and does not include space.

Defaults N/A.

Command Mode Global configuration mode.

Usage Guide 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.

Configuration 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.

Platform Description

N/A.

rmon collection history

Use this command to log the history of an Ethernet interface. The **no** form of this command cancels the logging.

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history *index*

Parameter Description

Parameter	Description
index	The index number of the history control entry, in the range of 1 to 65535.
owner*ownername*	Set the entry ownername, in a character string composed of 1 to 64 characters, the character string is case sensitive and does not include space.
buckets *bucket-number*	Set the history table volume of the history control entry, (the maximum volume of the history control entry as *bucket-number)*, in the range of 1 to 65535.
interval *seconds*	Set the statistics period *seconds*, in range of 1 to 3600, in second.

Defaults

N/A.

Command Mode

Interface configuration mode.

Usage Guide

The RGOS allows you to modify the configured history information of the Ethernet network, including **owner, buckets**, and **interval**. However, the modification does not take effect immediately until the system records history at the next time.

Configuration Examples

The example below Logs the history of Ethernet port 1.

```
Ruijie(config)# interface fast-Ethernet 0/1
Ruijie(config-if)# rmon collection history  1 zhansan buckets 10 interval 10
```

Related Commands

Command	Description
rmon collection stats *index* [**owner** *owner-name*]	Add a statistical entry.

Platform Description

N/A.

rmon collection stats

Use this command to monitor an Ethernet interface. The **no** form of this command removes the configuration.

rmon collection stats *index* [**owner** *owner-string*]

no rmon collection stats *index*

Parameter Description

Parameter	Description
index	The index of the statistics information sheet, in range of 1 to 65535
owner *ownername*	Set the entry ownername, in a character string composed of 1 to 64 characters. The character string is case sensitive and does not include space.

Defaults

N/A.

Command Mode

Interface configuration mode.

Usage Guide

N/A

Configuration Examples

The example below enables monitoring the statistics of Ethernet port 1.

```
Ruijie(config)# interface fast-Ethernet 0/1
Ruijie(config-if)# rmon collection stats 1 zhansan
```

Related Commands

Command	Description
rmon collection history *index* [**owner** *owner-name*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history control entry.

Platform Description

N/A.

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** *description-string*] [**owner***owner-name*]

no rmon alarm *number*

Parameter Description

Parameter	Description
number	The index of the event list, in range of 1 to 65535
log	The event log. When the event is triggered, the system will record in the log.
description *description-string*	Set the event description information *description-string* in a character string composed of 1 to 64 characters.
owner *owner-name*	Set the entry ownername, in a character string composed of 1 to 64 characters. The character string is case sensitive and does not include space.

Defaults

N/A.

Command Mode

Global configuration mode.

Usage Guide

Configuration 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.

Platform Description

N/A.

show rmon alarm

Use this command to show the rmon alarm table.

show rmon alarm

Parameter

Parameter	Description

Description

N/A.	N/A.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration 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.

Platform Description N/A.

show rmon event

Use this command to show the event information

show rmon event

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 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
```

Related Commands

Command	Description
rmon event *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	Add an event entry.

Platform Description N/A.

show rmon history

Use this command to show the history information.

show rmon history

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Command Mode N/A.

Usage Guide N/A.

Configuration Examples

The example below shows the history information.

```
Ruijie#  show rmon history
rmon history control table:
                index = 1
                interface = FastEthernet 0/1
                bucketsRequested = 10
                bucketsGranted = 10
                interval = 1800
                owner = zhangsan
                stats = 1

rmon history table:
                index = 1
                sampleIndex = 198
                intervalStart = 0d:14h:0m:47s
                dropEvents = 0
                octets = 67988
                pkts = 726
                broadcastPkts = 502
                multiPkts = 189
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
```

Related Commands

Command	Description
rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history control entry.

Platform Description

N/A.

show rmon statistics

Use this command to show the statistics.

show rmon statictics

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 shows the statistics.

```
Ruijie#  show rmon statistics
ether statistic table:
                index = 1
                interface = FastEthernet 0/1
                owner = zhangsan
                status = 0
                dropEvents = 0
                octets = 1884085
                pkts = 3096
                broadcastPkts = 161
                multiPkts = 97
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 1200
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 128
                packets65To127Octets = 336
                packets128To255Octets = 229
                packets256To511Octets = 3
                packets512To1023Octets = 0
                packets1024To1518Octets = 1200
```

Related Commands

Command	**Description**
rmon collection stats *index* [**owner** *owner-string*]	Add a statistical entry.

Platform Description N/A.

NTP Configuration Commands

debug ntp

Use this command to show the NTP debugging information. Use the **no** form of this command to turn off the debugging switch.

debug ntp

no debug ntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults Disabled.

Command mode Privileged EXEC mode.

Usage Guide To carry out the NTP function debugging, output necessary debugging information to implement the failure diagnosis and troubleshooting by this command.

Configuration Examples The example below enables the NTP debugging switch.

```
Ruijie(config)#debug ntp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

no ntp

Use this command to disable the NTP synchronization service with the time server and clear all NTP configuration information.

no ntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the NTP service is disabled.

Command mode

Global configuration mode.

Usage Guide

By default, the NTP function is disabled. However, once the NTP server or the NTP security identification mechanism is configured, the NTP function will be enabled.

Configuration Examples

The configuration example below disables the NTP service.

```
Ruijie(config)#no ntp
```

Related Commands

Command	Description
ntp server	Specify a 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	Not only allow to request for the time of and control the local NTP service, but also allow the time synchronization of the local and the peer.
serve	Allow to request for the time of and control the local NTP service only, the time synchronization of the local and the peer is not allowed.
serve-only	Allow to request for the time of local NTP service only.
query-only	Allow to control and search for the local NTP service.
access-list-number	The IP access control list number, in the range of 1-99 and 1300-1999.
access-list-name	The IP access control list name.

Defaults

No NTP access control rule has been configured by default.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure the access control priority of the ntp service. NTP services access control function provides a minimal security measures (more secure way is to use the NTP authentication mechanism).

When an access request arrives, NTP service matches the rules in accordance with the sequence from the smallest to the largest to access restriction, and the first matched rule shall prevail. The matching order is peer, serve, serve-only, query-only.

If you do not configure any access control rules, then all accesses are allowed. However, once the access control rules are configured, only the rule that allows access can be carried out.

Caution

Control query function is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

Configuration Examples

The following example shows how to allow the peer device in acl1 to control the 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	Create the IP access control list.

Platform Description

N/A

ntp authenticate

Use this command to enable NTP authentication globally. Use the **no** form of this command to disable this function.

ntp authenticate

no ntp authenticate

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled.

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 the trusted key specified by **ntp authentication-key** and **ntp trusted-key**.

Configuration Examples

After an authentication key is configured and specified as the global trusted key, enable the authentication mechanism.

```
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	Set the global authentication key.
ntp trusted-key	Configure the global trusted key.

Platform Description

N/A

ntp authentication-key

Use this command to configure a global NTP authentication key for the NTP server. Use the **no** form of this command to cancel the global NTP authentication key.

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

no ntp authentication-key *key-id*

Parameter Description

Parameter	Description
key-id	Key ID, ranging from 1 to 4294967295.
key-string	Key string
enc-type	(Optional) Whether this key is encrypted, where, 0 indicates the key is not encrypted, 7 indicates the key is encrypted simply.

Defaults

N/A

Command mode

Global configuration mode.

Usage Guide

Configure the global authentication key and adopt **md5** for encryption. Each key presents the unique *key-id* identification. Customers can use the **ntp trusted-key** to set the key of *key-id as* the global trusted key.

The upeer limit of the keys is 1024. However, each server can only support 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	Enable the global security identification mechanism.
ntp trusted-key	Configure the global trusted key.
ntp server	Specify a NTP server.

Platform Description

N/A

ntp disable

Use this command to disable the function of receiving the NTP message on the interface.

ntp disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The NTP message is received on the interface, by default.

Command mode

Interface configuration mode.

Usage Guide

The NTP message received on any interface can be provided to the client to carry out the clock adjustment. The function can be set to shield the NTP message received from the corresponding interface.

Caution

The interface that is configured with this command can receive and send IP packets. No this command is configured on other interfaces.

Configuration Examples

The configuration example below disables the function of receiving the NTP message 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 configure the local time as the NTP master (the local time reference source is reliable), providing the synchronizing time for other devices. Use the **no** form of this command to cancel the NTP master settings.

ntp master [*stratum*]

no ntp master

Parameter Description

Parameter	Description
stratum	Specify the stratum where the local time is, in the range of 1-15. The default stratum is 8.

Defaults

No NTP master is configured, by default.

Command mode

Global configuration mode.

Usage Guide

In general, the local system synchronizes the time from the external time source directly or indirectly. However, if the time synchronization of local system fails for the network connection trouble, etc., use the command to set the reliable reference source of the local time, providing the synchronized time for other devices.

⚠ Caution

Once set, the system time cannot be synchronized to the time source with higher stratum. Using this command to set the local time as the master (in particular, specify a lower stratum value), is likely to be covered by the effective clock source. If multiple devices in the same network use this command, the time synchronization instability may occur due to the time difference between the devices.

⚠ Caution

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 bias.

Configuration Examples

The configuration example below configures the reliable local time reference source and set the time stratum 12:

```
Ruijie(config)# ntp master 12
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

ntp server

Use this command to specify a NTP server for the NTP client. Use the **no** form of this command to delete the specified NTP server.

ntp server *ip-addr* [**version** *version*] [**source** *if-name*] [**key** *keyed*] [**prefer**]

no ntp server *ip-addr*

Parameter Description

Parameter	Description
ip-addr	Set the IP address of the NTP server.
version	(Optional) Specify the version (1-3) of NTP, NTPv3 by default.
if-name	(Optional) Specify the source interface from which the NTP message is sent (L3 interface).
keyid	(Optional) Specify the encryption key adopted when communication with the corresponding server.
prefer	(Optional) Specify the corresponding server as the prefer server.

Defaults No NTP server is configured, by default.

Command mode Global configuration mode.

Usage Guide At present, our system only support clients other than servers, and the upper limit of supported synchronous servers are 20.

To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server.

In the same condition (for instance, precision), the prefer clock is used for synchronization.

It should be noted that the configured interface is that configured with the IP address and can communicate with the corresponding NTP server when you configure the source interface of the NTP message.

Configuration Examples The configuration example below configures the equipment in the network as NTP server.

For IPv4: `Ruijie(config)# ntp server 192.168.210.222`

For IPv6: `Ruijie(config)# ntp server 10::2`

Related Commands

Command	Description

no ntp	Disable the NTP service function.

Platform Description

N/A

ntp trusted-key

Use this command to set a key at the global trusted key.

ntp trusted-key *key-id*

no ntp trusted-key *key-id*

Parameter Description

Parameter	Description
key-id	Global trusted key ID, ranging from 1 to 4294967295.

Defaults

N/A

Command mode

Global configuration mode.

Usage Guide

The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

Configuration Examples

The following configures an authentication key and sets it as the corresponding server trusted key.

```
Ruijie(config)#ntp authentication-key 6 md5 wooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp server 192.168.210.222 key 6
```

Related Commands

Command	Description
ntp authenticate	Enable the security authentication mechanism.
ntp authentication-key	Set the NTP authentication key.
ntp server	Specify a NTP server.

Platform Description

N/A

ntp update-calendar

Use this command to update the calendar for the NTP client using the synchronization time of the external time 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

By default, update the calendar periodically is not configured.

Command mode

Global configuration mode.

Usage Guide

By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

Configuration Examples

The following configures the NTP update calendar periodically.

```
Ruijie(config)# ntp update-calendar
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show ntp status

Use this command to show the NTP information.

show ntp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

If the NTP service of the system is enabled, show current NTP information. This command will not print any information before the synchronization server is added for the first time.

Configuration Examples

The example below shows the NTP information of current system.

```
Ruijie(config)#show ntp status
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

SNTP Configuration Commands

sntp enable

Use this command to enable the SNTP function. Use the **no** form of this command to restore the default value.

sntp enable

no sntp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Disabled

Command mode

Global configuration mode.

Usage Guide

This command shows the parameters of SNTP.

Configuration Examples

```
Ruijie(config)# sntp enable
```

Related Commands

Command	Description
show sntp	Show the SNTP configuration.
clock update-calendar	Synchronize the software clock with the hardware clock.
clock set	Set 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 interval *seconds*

no sntp interval

Parameter

Parameter	Description

Description

seconds	Synchronization interval in 60 to 65535 seconds

Defaults

1800s

Command mode

Global configuration mode.

Usage Guide

The **show sntp** command shows the parameters of SNTP.

Note that the set interval will not take effect immediately. To this end, execute the **sntp enable** command after setting the interval.

Configuration Examples

```
Ruijie(config)# sntp interval 3600
```

Related Commands

Command	Description
sntp enable	Enable SNTP.
show sntp	Show 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. Since the SNTP protocol is completely compatible with the NTP protocol, you can configure the SNTP server as the public NTP server on the Internet.

sntp server *ip-address*

no sntp server

Parameter Description

Parameter	Description
ip-address	The IP address of the NTP/SNTP server.

Defaults

No NTP/SNTP server is configured.

Command mode

Global configuration mode.

Usage Guide

The **show sntp** command shows the parameters of SNTP.

Configuration

```
Ruijie(config)# sntp server 192.168.4.12
```

Examples

Related Commands

Command	Description
show sntp	Show the SNTP configuration.
sntp enable	Enable SNTP.

Platform Description N/A

show sntp

Use this command to show the parameters of SNTP.

show sntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command mode Privileged EXEC mode.

Usage Guide This command shows the parameters of SNTP.

Configuration Examples

```
Ruijie# show  sntp
SNTP state           : Enable
SNTP server          : 192.168.4.12
SNTP sync interval    : 60
Time zone             : +8
```

Related Commands

Command	Description
sntp enable	Enable SNTP.
show sntp	Show the SNTP configuration.

Platform Description N/A

SPAN Configuration Commands

monitor session

Use this command to create a SPAN session and specify the destination port (monitoring port) and source port (monitored port). The **no** form of the command is used to delete the session or delete the source port or destination port separately.

monitor session *session_number* { **source interface** *interface-id* [**both** | **rx** | **tx**] | **destination interface** *interface-id* { **encapsulation | switch** } | **mac** { **source** *mac-addr* | **destination** *mac-addr* } [**both** | **rx** | **tx**] } [**acl** *name*]

no monitor session *session_number* [**source interface** *interface-id* [**both** | **rx** | **tx**] | **destination interface** *interface-id* { **encapsulation | switch** }] | **mac** { **source** *mac-addr* | **destination** *mac-addr* } [**both** | **rx** | **tx**] [**acl** *name*]

no monitor session all

Parameter Description

Parameter	Description
session_number	SPAN session number
source interface *interface-id*	Specify the source port. *interface-id*: interface ID, which can be physical interface, not SVI.
destination interface *interface-id*	Specify the destination port. *interface-id*: interface ID, which can be physical interface, not SVI.
mac source *mac-addr*	The source MAC address of the mirrored frame.
mac destination *mac-addr*	The destination MAC address of the mirrored frame.
both acl *name*	Monitor the inbounding and outbounding frames simultaneously. **acl** *name/id* of monitored flow
rx	Monitor only the inbounding frames.
tx	Monitor only the outbounding frames.
all	Delete all sessions.
encapsulation	Support the encapsulation function for the monitored port. Once this function is enabled, the tag of the mirrored frame is peeled off forcibly. This function is disabled by default.
switch	Enable switching on the mirroring destination port. It is disabled by default.

Defaults N/A

Command mode Global configuration mode.

Usage Guide Both switch port and routed port can be configured as the source port or destination port. The SPAN session has no effect on the normal operation of the equipment. You can configure a SPAN session on disabled ports. However, the SPAN does not work unless you enable the source and destination ports.

A port cannot be configured as the source port and the destination port at the same time.

You will remove the whole session if you do not specify the source port or the destination port.

Use **show monitor** to display SPAN session status.

Caution

Session 1 supports global port mirroring crossing line cards. To configure the SPAN crossing the line cards, only the session 1 can be used.

Configuration Examples

The example below describes how to create a SPAN session: session 1: If this session is set previously, clear the configuration of current session 1 firstly, and then set the frame mapping of port 1 to port 8.

```
Ruijie(config)# no monitor session 1
Ruijie(config)# monitor session 1 source interface gigabitEthernet 1/1 both
Ruijie(config)# monitor session 1 destination interface gigabitEthernet 1/8
```

Related Commands

Command	Description
show monitor	Use this command to display the SPAN configurations.

Platform Description

N/A

show monitor

Use this command to display the SPAN configurations.

show monitor [**session** *session_number*]

Parameter Description

Parameter	Description
session *session_number*	SPAN session number.

Defaults

All SPAN sessions are displayed by default.

Command mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

This example shows how to use **show monitor** to display SPAN session 1:

```
Ruijie# show monitor session 1
```

```
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

Related Commands

Command	Description
monitor session	Specify a SPAN session and the destination port (mirroring port) and the source port (mirrored port).

Platform Description

N/A

RSPAN Configuration Commands

monitor session

Use this command to create an RSPAN session and specify a destination port (monitoring port), source port (monitored port) or reflector port. Use the **no** form of this command to delete the session or remove the source port, destination port or reflector port separately.

Set attributes for the mirroring device:

monitor session *session_num* { **remote-destination** | **remote-source** }

no monitor session *session_num* { **remote-destination** | **remote-source** }

Set destination mirroring:

monitor session *session-num* **destination remote vlan** *vlan-id* [**reflector-port**] **interface** *interface-name* [**switch**]

no monitor session *session-num* **destination remote vlan** *vlan-id* [**reflector-port**] **interface** *interface-name* [**switch**]

Set remote source mirroring:

monitor session *session-num* **source interface** *interface-name* [**rx** | **tx** | **both**]

no monitor session *session-num* **source interface** *interface-name* [**rx** | **tx** | **both**]

Set the mirroring reflector port:

monitor session *session-num* **destination remote vlan** *vlan-id* **reflector-port interface** *interface-name* [**switch**]

no monitor session *session-num* **destination remote vlan** *vlan-id* **reflector-port interface** *interface-name* [**switch**]

Delete the session:

no monitor session session-num

Parameter Description

Parameter	Description
session-num	Session number.
vlan-id	Remote span vlan id.
interface-name	Interface name

Defaults

No mirroring configuration by default.

Command Mode

Global configuration mode.

Usage Guide

Enter the **end** command or press **Ctrl+C** to return to privileged EXEC mode.

Enter the **exit** command to return to global configuration mode.

Configuration Examples

The following example configures the source switch:

```
Ruijie(config)# monitor session 2 remote-source
Ruijie(config)# monitor session 2 source interface gigabitEthernet 1/2
Ruijie(config)# monitor session 2 destination remote vlan 7 interface
gigabitEthernet 1/3 switch
Ruijie(config)# monitor session 2 destination remote vlan 7 reflector-port
interface gigabitEthernet 1/1 switch
```

The following example configures the destination switch:

```
Ruijie(config)#monitor session 2 remote-destination
Ruijie(config)#monitor session 2 destination remote vlan7 interface
gigabitEthernet1/1 switch
```

Related Commands

Command	Description
show monitor	Show mirroring session information.

Platform Description

N/A

remote-span

Use this command to enable the remote port mirroring function in a VLAN. Use the **no** form of this command to disable this function.

remote-span

no remote-span

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

Disabled.

Command Mode

VLAN configuration mode.

Usage Guide

Enter the **end** command or press **Ctrl+C** to return to privileged EXEC mode.

Enter the **exit** command to return to global configuration mode.

Configuration Examples

```
Ruijie(config)# vlan 5
Ruijie(config-vlan)# remote-span
```

Related Commands

Command	Description
show vlan	Show VLAN information.

Platform Description	N/A